Version: 20130502b

Red Team – Attacker Playbook

Red Team (Attackers) – Discussion Topics	**Team Conclusions:**

What is your objective:
• Theft of:
  • Intellectual Property/Trade Secrets
  • Personally Identifiable Information (e.g., for identity theft)
  • Financial Information (e.g., for financial theft)
  • Denial of Business Operations (e.g., deny customer access to resources)
  • Disturbance of Electrical Grid (e.g., cause blackout)
• Sabotage (e.g., property destruction, human casualties, etc.)
	Objective (Pick one)
	○ Theft of IP/Secrets Theft of PII
	○ Theft of Financial Info Denial of Bus Ops
	○ Grid Disturbance
	○ Sabotage
	
	Notes:

What resources would you attack: • Business Assets (e.g., systems that sore intellectual property, financial information, trade secrets, etc.) • Power Generation Assets (e.g., transformers, generators, etc.) • Safety, Security or, Emergency Response Systems (e.g., disable security systems, prevent safety system function, challenge response, etc.)	What resources would you attack? (Pick one) ○ Business Assets ○ Power Generation Assets ○ Safety, Security or, Emergency Response Systems Notes:
Are your decisions influenced by regulatory requirements, laws, or other public policy?	Are you influenced by policy? (Pick one) ○ Yes ○ No Notes:
How do you allocate resources to prepare for attack: • Reconnaissance (e.g., determine victim assets, defenses, and detection capabilities, etc.) • Attack (e.g., compromise computers, gain unauthorized access, breach security measures, execute denial of services, etc.) • Exploitation (e.g., harvest PII/financial data/trade secrets, destroy assets or equipment, etc.)	Allocation of resources to recon, attack, or exploit? (Prioritize in order of 1, 2, or 3; 1 is high priority, 3 is low priority) ❖ Reconnaissance ❖ Attack ❖ Exploitation Notes: