Assignment & Lab Centers of Gravity (COG) Summary
created by Damsith Marasinghe

Objective

My primary objective is launching a cyber attack on Transformers, Power Lines and Turbine/Generators on ABC industrial power plant in the United States.

Operation Design

The following description relates to the Advanced Turbine Systems plant (ATS) operational design aspect. The state of the art 240-MW 501F Reference Plant includes changeable accepted design features that minimize design changes usually required to tailor the plant to site specific restrictions. The power supply of both plants contains one combustion turbine and one multi-pressure steam turbine. The 240MW Reference Plant is a multishaft design. The ATS Plant uses a single shaft design with a shared generator between the combustion turbine and steam turbine. Both plants are fueled by natural gas and utilize mechanical draft cooling towers. The ATS plant generates considerably more power at a higher efficiency than the 240 MW Reference Plant, primarily because of the added power and performance of the ATS combustion turbine and the elevated throttle pressure and reheat temperatures of the steam turbine.
As I could see, information technology (IT) and operational technology (OT) networks are air-gapped, meaning there was no direct link between the two entities. Advances in automation have resulted in merged systems that present a clear danger. As Malicious actor I could gain access to the IT infrastructure and I may also be able to compromise and disrupt the OT systems required to generate power. So the Transformers, Power Lines, Steam/Combustion Turbines, Generator that I identified in the Carver Method as critically vulnerable resources that could undergo a cyber attack of some form. Hackers are always searching for systems with weak authentication that can be easily compromised. Network-accessible devices with weak or default passwords can serve as a gateway to more critical systems. The lack of dedicated IT teams can make it difficult to promptly install software security patches and updates. This allows hackers to exploit known security vulnerabilities repeatedly. I will exploit all these weaknesses.
Using my strategic plans as a hacker, I will try to hack into ABC Industrial Power plant by hacking into the main frame of the power plant as it is more centralized. I will hack into the system by there security systems wifi network within powered grid and shutting down the Turbines which supplies power to each region of the States.

Identfying COG

I have identified the Transformers, Power Lines, Steam/Combustion Turbines, and Generator (that I identified in the Carver Method) as critically vulnerable resources that could undergo a cyber attack of some form. Once you attack these critically vulnerable

resources, the power plant will shut down as these are the resources that generate power in the ABC industrial power plant.

CARVER SCALE and Explanation

A value is selected for each of the Carver matrix factors. Criticality is defined as the volume of enemy threats (maximum 20). Accessibility is the availability of the power plant to the enemy (maximum 30). The fuel consumption of the power plant is considered Recuperability (maximum 5). The age of the power plant is considered Vulnerability (maximum 20). The production capacity of the power plant is taken as the Effect (maximum 40). Finally, the location of the power plant is considered Recognizability (maximum 8). It should be noted that the factor values have been determined through extensive research and conform to the opinion of the elite.

Target Components	C	A	R	V	E	R	Total
Transformers	18	29	4	18	38	7	102
Power lines	19	25	2	16	32	4	98
Steam/CombustionTuribine	19	28	1	15	3	4	70
Generator	17	24	3	14	2	6	66
Docks and Oil Pumps	5	6	1	3	3	4	23
Blowers	5	3	2	3	3	3	22
Boiler	6	4	2	3	2	4	21
Pre-heater and Pumps(Fuel)	8	3	4	3	1	2	21
Switching Station	4	6	3	3	2	1	19
Pre-heater and Pumps	3	3	4	3	4	2	19
Water Filters and Pumps	7	2	1	2	4	2	18
Bargers	3	4	1	3	2	4	17
Storage Tanks	2	2	1	3	4	5	17
Ion Filiter	4	3	3	2	3	1	16
Air intake	2	4	1	2	3	4	16

I have identified the following Critical Vulnerabilities as in the above Carver Matrix:

- Transformers
- Power Lines
- Steam / Combustion Turbines
- Generator

REFERENCES

https://www.osti.gov/servlets/purl/828617

https://archive.conscientiabeam.com/index.php/13/article/view/2965/6419

https://www.helpnetsecurity.com/2021/05/13/power-plants-security-threats/