INTELLIGENCE METHODOLOGIES

REFERENCE SHEET

Software Engineering Institute | Carnegie Mellon University

RED TEAMING

Summary:
A red team is an independent group that thinks from the perspective of an organization's adversaries. Red teaming can help reveal gaps and weaknesses in an organization's existing processes or security and help in creating strategies to overcome possible exploits. Red teaming is most beneficial if done before deploying new security strategies or implementing new organizational processes.

How it is done:
Red team exercises examine what information an adversary would want, how the adversary could obtain this information, and what impact the loss of this information would have on the organization and the adversary.

Required Tools:
Red teams utilize tools that would be available to an organization's adversaries, including access to hardware, software, and open source.

Required Data:
Red teams utilize data that would be available to an organization's adversaries. This data includes open source information and information openly available, such as documents left in printers, thrown away, or left in view on a desk.

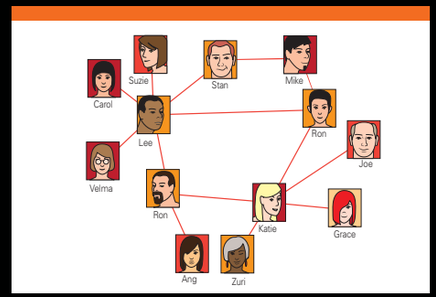
Expected Outcome:
Red teams can help organizations identify their vulnerabilities (physical or network-based) as well as potential damages or losses that could result from exploitation of these vulnerabilities. Once vulnerabilities are identified, organizations can modify security strategies and organizational processes to prevent exploitation.

References:
Red Team Handbook. (2011). University of Foreign Military and Cultural Studies.

SOCIAL NETWORK ANALYSIS

Summary:
Social network analysis (SNA) examines relationships. It helps organizations determine entities' roles, relationships, and levels of influence over others. SNA should be performed after sufficient information is collected on the entities being compared.

How it is done:
SNA is performed by examining links between related entities. Relationships can include: familial, business, connections on social media, ideological, or physical location. Typically, these links are represented in a visual social network diagram. Some software automates the link generation process based on user input or imported data while other software requires links to be drawn manually.



Required Tools:
Several software tools help perform SNA, including Ora, Maltego, i2 Analyst's Notebook, Palantir, and Gephi. SNA could also be performed without software.

Required Data:
SNA requires information about the relationships between entities. For example, if an organization is examining the organizational structure of a cyber crime group, the organization may collect information on communications between members via social media, geographic information on group members, or group members' educations and employment.

Expected Outcome:
SNA can help organizations determine ties between entities as well as which entities influence others.

References:
Hanneman, R. A., & Riddle, M. (2005). Introduction to Social Network Methods: Riverside, CA: University of California, Riverside.
Wheaton, K. J. (2008, December 11). Top 5 Intelligence Analysis Methods: Social Network Analysis (#3). Sources And Methods.

IMPACT V. PROBABILITY GRAPH

Summary:
An impact v. probability graph examines the probability an event will occur and the impact that event would have on an organization. As this methodology aids in prioritizing potential risks, organizations should gather information on threats before using this methodology.

How it is done:
This graph requires two axes, one labeled "Probability" and the other labeled "Impact." The point where these axes meet is considered the lowest probability of the event occurring and the lowest impact the event will have; the probability and impact increase moving farther from the origin. Probability is defined as the risk that an event may occur while impact is defined as the negative effect an event will have on an organization. Each potential threat then is plotted on the graph according to its probability and impact. Threats that are toward the top right corner are most severe while threats in the bottom left corner are low level threats.

Required Tools:
This methodology can be performed using a pen and paper or whiteboard, but software may be helpful. Organizations may find spreadsheet and graphing software such as Microsoft Excel useful, especially if the organization wishes to weigh a certain factor (such as actor sophistication). Additionally, organizations may employ binary risk analysis to help measure potential impacts and probabilities.

Required Data:
Organizations should gather information on potential threats, including the probability of an event occurring and the impact that event would have on the organization. To examine probability, organizations may collect information on potential threat actor's capabilities for performing an attack or that actor's intent to perform the attack. This information may include the tools and software available to the actor or the actor's past history performing attacks. To examine impact, an organization may collect information on the monetary costs of an attack or the attack's impact on reputation. This information may include the cost if a server is down for an extended period, the cost of implementing new defenses for future threat mitigation, or the potential loss of customers.

Expected Outcome:
An impact v. probability graph can help an organization prioritize threats based on probability of occurrence and potential impact. Additionally, this methodology can help organizations to monitor threats for change. Prioritizing and monitoring threats allows organizations to wisely invest cyber security resources to mitigate the most severe threats to a network.

References:
LUMA Institute, & LUMA Institute. (2012). Innovating for People: Handbook of Human-Centered Design Methods. Pittsburgh, Pennsylvania: LUMA Institute, LLC. Risk Impact/Probability Chart. (2013). Mind Tools.

AFFINITY CLUSTERING

Summary:
Affinity clustering is a technique for sorting items according to similarity. Affinity clustering is performed after information is collected to reveal patterns or gaps.

How it is done:
To perform affinity clustering, individual data points are captured in a common workspace. These data points then are grouped into clusters based on similarity and the data clusters are assigned labels.

Required Tools:
Affinity clustering can be performed using cards or sticky notes for each piece of information, but mind mapping tools may be helpful. Mind mapping tools include MindMeister, Mindomo, or Microsoft Visio.

Required Data:
The specific data required depends on the relationship being examined. For example, if an organization is examining tools used by different cyber crime organizations to obtain personal information, they should gather information such as the name of the tool, what other activities the tool can be used for, what operating system the tool runs on, and what type of information was stolen.

Expected Outcome:
Affinity clustering can help organizations determine relationships and patterns among collected information. Small clusters may indicate a lack of data, or outliers from more significant data. Larger clusters may suggest trends, indicate an over-collection of a particular set of data, or identify key areas for analysis. For example, an organization may determine that most cyber crime organizations prefer to target a specific vulnerability or identify that certain types of personal information are rarely stolen.

References:
LUMA Institute, & LUMA Institute. (2012). Innovating for People: Handbook of Human-Centered Design Methods. Pittsburgh, Pennsylvania: LUMA Institute, LLC.

MULTI-CRITERIA DECISION MAKING

Summary:
Multi-criteria decision making (MCDM) evaluates possible courses of action (COAs) against an established set of criteria. Since MCDM requires an organization to specify criteria that should be met and possible COAs, MCDM is useful during the decision-making process or at the end of an analysis phase.

How it is done:
MCDM is performed using a matrix with one axis containing criteria and the other containing possible COAs. The COAs then are given a score from one to three based on how well that COA satisfies the criteria, with a score of one given to a COA that does not effectively satisfy the criteria and three given to a COA that effectively satisfies the criteria. After each criteria is examined, each COA's scores are added up and the COA with the highest score best satisfies all given criteria.

	Raw Score				Weighted Score		
	Option A	Option B	Option C	Criteria Weight	Option A	Option B	Option C
Cost	4	8	3	1	4.0	8.0	3.0
Quality A	6	9	4	1	6.0	9.0	4.0
Quality B	8	7	5	0.8	6.4	5.6	4.0
Feature A	5	6	4	1	5.0	6.0	4.0
Feature B	3	8	3	0.5	1.5	4.0	1.5
Feature C	2	9	8	0.8	1.6	7.2	4.8
			Total Weighted Score		**24.5**	**39.8**	**21.3**

Required Tools:
Although MCDM matrices can be drawn by hand, some organizations may find spreadsheet software helpful.

Required Data:
MCDM requires a list of criteria an organization would like a course of action to met as well as a list of possible courses of action. For example, if an organization is determining which network analysis tool to use, each COA may be a different tool while criteria may include actions the organization would like the tool to perform or other requirements (such as low cost).

Expected Outcome:
MCDM can help organizations determine a course of action that best satisfies a list of established criteria.

References:
Wheaton, K. J. (2008, December 12). Top 5 Intelligence Analysis Methods: Multi-Criteria Decision Making Matrices/Multi-Criteria Intelligence Matrices (#2). Sources And Methods.