SAND2008-7611P

Identify Relevant Target Metrics

Targeted metrics

Types of Security Metrics

(Six Empirical Classes for Red Teaming)

"The universe of metrics is large, even for measuring security."

- Attack-based metrics
- Vulnerability-based metrics
- Consequence-based metrics
- Adversary-based metrics
- Protection-based metrics
- Threat-based metrics

Attack Metrics

Attack-based metrics describe the capabilities and commitment required to undertake a given attack successfully.

- Attack-based metrics
  - imply detailed understanding of the process necessary to perform an attack - the path from adversary discovery to adversary goal completion, and
  - have a significant degree of overlap with *adversary metrics.*
- Example commitment factors*
  - intensity (e.g., willing to risk going to prison),
  - stealth (e.g., detection unacceptable) , and
  - time (e.g., slow vs. fast).

*Think of these in both adversary <u>and</u> attack terms.

- Attack-based metrics derived from capabilities include those for attack
  - discovery (e.g., knowledge),
  - development (e.g., R&D program for sophisticated exploits), and
  - execution (e.g., access).

V Vulnerability Metrics

(aka Weakness-Based Metrics)

Vulnerability-based metrics count vulnerabilities found or weaknesses discovered.

- Examples include
  - Boolean (yes/no - is there a vulnerability?),
  - percentage of vulnerable platforms, and
  - reachability (is the weakness within reach of adversaries?).
- Counting vulnerabilities found or weaknesses discovered is made more relevant when used with adversary metrics to show which vulnerabilities could be exploited by adversary (or adversary model)
- One problem is overcoming unknown vulnerabilities:

"There are known knowns. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don't know. But there are also unknown unknowns. There are things we do not know we don't know."

- Donald Rumsfeld 2002, February 12

C Consequence Metrics

Consequence-based metrics describe or measure the consequences that attend a successful attack.

- Examples include
  - number of deaths,
  - system downtime, and
  - nightmare consequences*.
- An approach to estimating a target's vulnerability of undesirable consequences is
  - brainstorm attacks, apply filters (key filter is adversary), and analyze countermeasures, then
  - measure security by determining what consequences cannot occur under adversary attack.

* The IDART™ red teaming methodology identifies the need to elicit nightmare consequences from sponsors during red team planning. Sometimes, during the course of an assessment, the red team identifies other previously unknown consequences that are of greater magnitude than what the customer has identified.

Ad Adversary Metrics

Adversary-based metrics describe the adversary model the red team uses during the red team process.

- Example adversary commitment factors
  - intensity – stealth – time
- Example adversary resources
  - number of team personnel,
  - knowledge (technology, cyber, kinetic, etc.),
  - skill level,
  - quality and sophistication of tools, and
  - insider access.
- Adversaries may acquire specialized resources as required
- Consider money to be a resource multiplier, and not necessarily a stand alone resource
- Adversary metrics have significant overlap with *attack metrics*

P Protection-Based Metrics

Protection-based metrics count or measure protection systems (extant or posited as countermeasures).

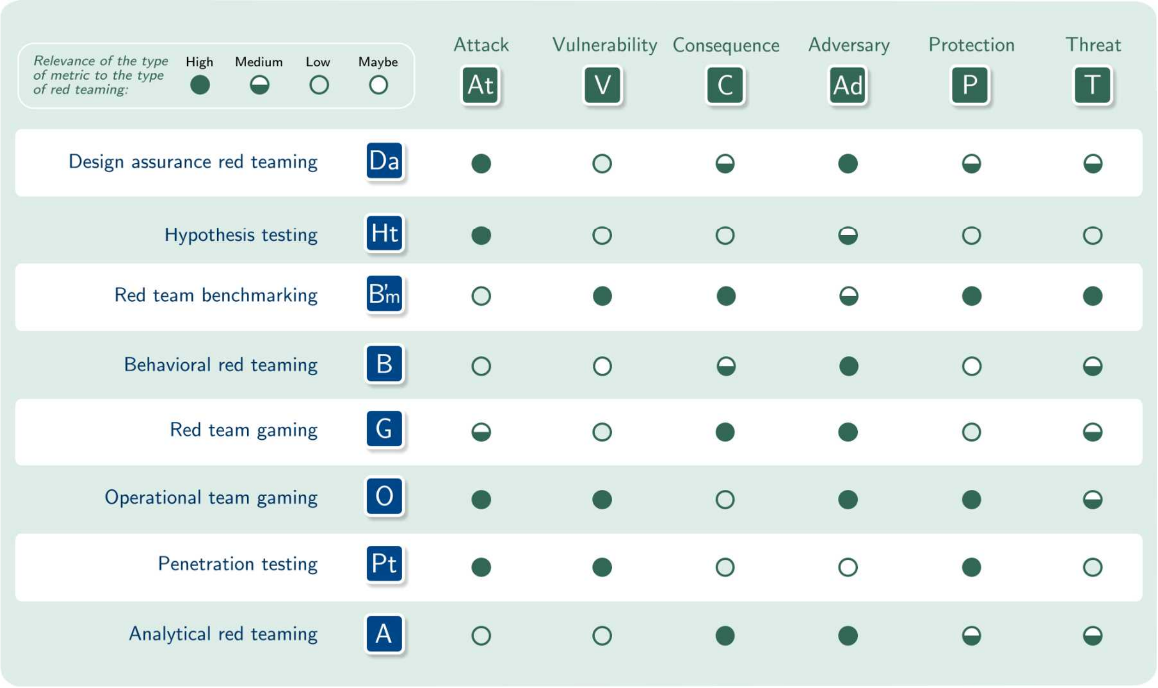
- If unknowns can't be counted, count the known - protections.
- Examples include
  - number of security layers,
  - number of systems protected, and
  - number of compromises (e.g., daily, quarterly, annually).
- P-b metrics are perhaps most useful in conjunction with other metrics, particularly attack metrics
- An example of the non-measurable is the mapping between a known protection system and a set of unknown weaknesses

T Threat-Based Metrics

Threat-based metrics describe the degree of threat and are calculated using combinations of the other metrics cited here.

- Threat-based metrics imply a composite calculation using *consequence, vulnerability, protection*, and *adversary-based metrics*
- T-b metrics are calculated from the defender's point of view – the assets to be protected are those important to the defender, not necessarily those important to real adversaries
- Examples include
  - expected cost to repair damage,
  - number of systems expected to be affected, and
  - estimated mean time to restore services.

Identify Relevant Target Metrics



Relevance of the type of metric to the type of red teaming: High ● Medium ◒ Low ○ Maybe ○

		Attack At	Vulnerability V	Consequence C	Adversary Ad	Protection P	Threat T
Design assurance red teaming	Da	●	○	◒	●	◒	◒
Hypothesis testing	Ht	●	○	○	◒	○	○
Red team benchmarking	B'm	○	●	●	◒	●	●
Behavioral red teaming	B	○	○	◒	●	○	◒
Red team gaming	G	◒	○	●	●	○	◒
Operational team gaming	O	●	●	○	●	●	◒
Penetration testing	Pt	●	●	○	○	●	○
Analytical red teaming	A	○	○	●	●	◒	◒

- Use this table to help identify target metrics
- Eight types of red teaming are listed on the left*
- Six types of target metrics are listed on the top
- Make a list of the types that apply to your assessment
- Section 2 explores the types in more detail and techniques to use

Identification of metrics is part of red team planning (e.g., IDART™ method), but not necessarily part of RT4PM™ planning.

*Sandia's Red Teaming for Program Managers (RT4PM™) training identifies eight types of red teaming.

Questions?

Section One Exercise

- A homeowner wants to know how vulnerable they are to loss *(Understand the customer's business questions)*
  - The homeowner asks, “how secure is my home?”

  (Translate the customer's business questions to security questions)
  - To help answer this question, the homeowner hires a red team
- As the red team, you must determine which attack path is best (hint: “best” points to the need for metrics)
  - The red team assumes a burglar adversary model(s)
- To do so, the red team starts by asking, “what metrics should be used to determine if one attack is better than another?” *(Identify relevant target metrics)*

- **Exercise: Break into groups and determine what metrics your red team burglar(s) would use to determine which attack is best.**