Red Teaming Quick Reference Sheet

RT4PM Red Teaming for Program Managers

Designed to help you ...

1. Determine your need for red teaming
2. Specify what your red team should do
3. Identify the right red team
4. Plan to use your red teaming deliverables

This quick reference sheet is a component of Sandia's Red Teaming for Program Managers class.

- **Da** Design assurance
- **Ht** Hypothesis testing
- **Bm** Benchmarking
- **B** Behavioral red teaming
- **G** Gaming
- **O** Operational red teaming
- **Pt** Penetration testing
- **A** Analytical red teaming

These types of red teaming represent *empirical categories*, each based on one or more prototypical uses of red teams. These categories attempt to maximize the similarity of red team uses within each category and to minimize the similarity of uses between categories. But, some overlap is expected.

The description of each type given in this quick reference sheet provides a *black-box definition* to help program managers identify key issues and common difficulties. Real-world assessments often require hybrid approaches, drawing methods and concepts from one or more of these types.

1 Determine your need for red teaming

High ● *Medium* ◒ *Low* ○ *Maybe* ◌

	Da	Ht	Bm	B	G	O	Pt	A
Understand adversaries and operational environments, assess threats	◌	○	○	●	●	○	◒	○
Anticipate program risk, identify security assumptions, and support security decisions	○	○	◒	◒	●	◌	○	●
Explore and develop security options, policy, process, procedures, and impacts	◒	●	◒	○	○	◌	○	◒
Establish an in-house red team	○	○	○	○	●	◒	◒	○
Identify and describe consequential program security requirements	◒	●	◒	○	○	◌	○	○
Identify and describe consequential security design alternatives	●	●	●	○	○	◌	○	○
Measure security progress and establish security baselines	◒	○	●	◌	◌	○	○	◌
Understand how a system defeats adversaries	◒	◒	◒	◌	◌	○	●	◒
Explore security of future concepts of operation	○	○	◌	◒	●	●	◒	◌
Test and train operations personnel response to attack	◌	◌	◌	○	◒	●	●	◌
Identify and describe surprise, unintended consequences	●	○	◌	○	◒	○	●	◒

This list of security concerns is incomplete, and with experience a program manager or red team may add to it more specific security concerns.

13 Sept 2017

2 Specify what your red team should do

RT4PM Red Teaming for Program Managers

Design assurance red teaming

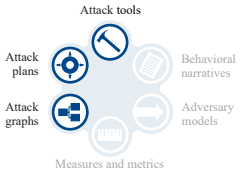
Da

Design assurance helps ensure a system will achieve its mission in hostile environments. It is usually performed with the cooperation of the development team and typically models goal-directed adversaries motivated to defeat the system's mission. Design assurance assessments do not require functional systems, and often the greatest benefits result from assessment of prototypes or even early design documentation.

Considerations:

- Engage the red team as early as possible in the design process
- Encourage the red team and development team to cooperate
- Include the red team in design reviews and planning activities
- Facilitate red team access to documentation or prototypes
- Consider adversaries beyond those identified at project start
- Provide for iterative red team assessments during design and implementation

Deliverables:



Cost Factors:

- Number of adversaries to be modeled
- Number of experiments or demonstrations
- Number of assessment iterations

Concept → *Retirement*

Red team hypothesis testing

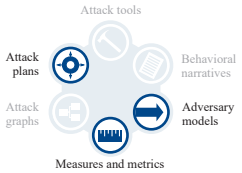
Ht

Hypothesis testing helps to confirm or reject a conjecture, whether formally or informally conceived, and to understand the merits of competing alternatives. Experiments designed to evaluate hypotheses frequently help determine the viability of proposed security measures. Hypothesis testing often involves multiple teams, including white and blue teams and often multiple red teams.

Considerations:

- Define hypotheses that can be confirmed or rejected
- Establish a measurement plan to collect required data
- Measure what can be meaningfully compared
- Make sure experiment plans are clear and well defined
- Make sure rules of engagement are not too limiting
- Consider conflicts of interest when building teams

Deliverables:



Cost Factors:

- Number of hypotheses
- Number of experiments
- Number of teams

Concept → *Retirement*

Red team gaming

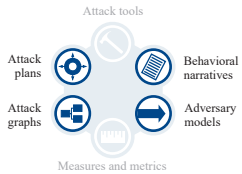
G

Gaming facilitates interactive, exploratory development of adversarial scenarios in a simulated environment. Unlike traditional gaming, red team gaming focuses more on the adversary's goals and activity than on the defender's mission. Games help to explore ideas, test operational concepts, challenge perspectives, and train staff. Gaming applies mainly to problems involving human decision making.

Considerations:

- Use to complement other forms of analysis
- Define research questions early in game development
- Explicitly link research questions to program goals
- Require game designers to document assumptions and design decisions
- Acquire players with real-world experience
- Provide for iterative game play when possible

Deliverables:



Cost Factors:

- Realism of game play
- Type of game (table-top exercise, board game, etc.)
- Simulation and computer support requirements

Concept → *Retirement*

Behavioral red teaming

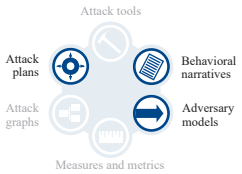
B

Behavioral red teaming records how a specific adversary might act in a given context. This can help analysts and designers assess what might deter or prevent an adversary from acting, distinguish malicious from routine behaviors, and determine meaningful attack indicators. Behavioral red teams often depend on subject matter experts and team members drawn from the adversary demographic.

Considerations:

- Define the adversary and the adversary's goal and context
- Make sure the red team models the adversary accurately
- Establish a measurement plan to collect required data
- Determine detail needed in narrative of adversary behavior
- Define operational security plan for red team activities and deliverables
- Consider methods of analyzing measures, metrics, and narratives

Deliverables:



Cost Factors:

- Number of adversaries
- Number of adversary goals and contexts
- Number of teams

Concept → *Retirement*

2 Specify what your red team should do

RT4PM Red Teaming for Program Managers

Red team benchmarking

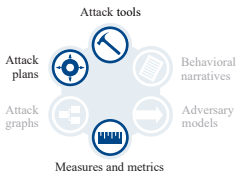
Bm

Benchmarking establishes a baseline for comparing system responses to adversary actions and helps measure progress of an implementation toward a security specification, progress of an implementation relative to an earlier benchmark, and measured security of one implementation relative to another. Security specifications used in benchmarking are often sensitive or even classified.

Considerations:

- Determine sensitivity and guidelines for using security specifications
- Establish a measurement plan for the benchmark
- Measure what can be compared meaningfully
- Define and document the benchmarking process
- Define the red team methodology to ensure consistent results
- Define and document method of comparing benchmarks

Deliverables:



Cost Factors:

- Number of benchmarks
- Number of red teams
- Number of assessment iterations

Concept → *Retirement*

Operational red teaming

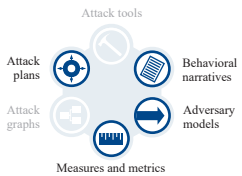
O

Operational red teaming models an active adversary within a live or simulated context. Operational red teams seek to defeat the target system's mission in realistic deployment environments. Operational red teaming helps to train staff, conduct testing and evaluation, validate concepts of operation, and identify vulnerabilities. Operational red teams will usually have less time than real-world adversaries to prepare.

Considerations:

- Match effort's fidelity with program requirements
- Carefully weigh and define rules of engagement
- Validate that red team acts within required constraints
- Obtain all required authorizations; identify and mitigate activity risks
- Consider establishing a standing operational red team or opposing force (OPFOR)
- Match existing scenarios with program's concept of operations (CONOPS)

Deliverables:



Cost Factors:

- Scope, scale, and complexity of target system
- Materials required to execute program
- Level of active response from blue team

Concept → *Retirement*

Analytical red teaming

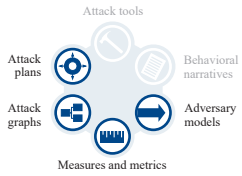
A

Analytical red teaming applies formal and mathematical methods to identify and evaluate the courses of action an adversary might take to achieve a mission. Most forms of analytical red teaming explore and model the potential attack space and reduce this space by comparing specific adversary models. Most analytical red teams do not perform field work but might use field data. Analysis often includes consideration of tactics, techniques, and procedures.

Considerations:

- Bound the team's objectives; do not allow the team to exceed its mission
- Err on the side of breadth rather than depth; depth is achieved through iteration
- Encourage teams to use structured methods and tools
- Prefer teams that employ proven and reusable methods
- Consider methods of validating analysis results

Deliverables:



Cost Factors:

- Scope, scale, and complexity of target system
- Degree to which team can draw from past efforts
- Simulation and computer support requirements

Concept → *Retirement*

Penetration testing

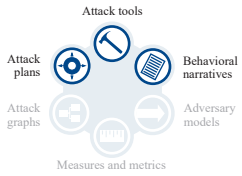
Pt

Penetration testing determines whether and by what methods a red team, possibly modeling a particular adversary, can defeat security controls designed to prevent unauthorized access or control of systems and data. Penetration tests help determine what access or control an insider, an outsider, or an outsider working with an insider may obtain. Penetration tests usually require functional systems and consider only what can be done at a given point in time.

Considerations:

- Determine need to model a particular adversary
- Determine whether red team has necessary skills and experience with similar systems
- Determine need for blue and white teams
- Clearly define and balance team roles and rules of engagement
- Obtain all required authorizations; identify and mitigate activity risks
- Determine whether team's method is sufficiently detailed to draw accurate conclusions

Deliverables:



Cost Factors:

- Scope, scale, and complexity of target system
- Safety or criticality of assets involved
- Number of teams

Concept → *Retirement*

3 Identify the right red team

RT4PM Red Teaming for Program Managers

Experience

- What is your experience red teaming?
- What is your experience red teaming programs like this one?
- How long has your red team existed?

Process

- What are your processes for red teaming?
- What resources are available to your team?
- What is in your reports? How are they structured?
- How do you reproduce the behavior of a particular adversary?
- What hardware and software tools do you use?
- How do you identify and mitigate risks posed by your assessment activities?
- What are your OPSEC practices?

Composition and Capability

- Who will be on the team?
- What is the proposed team's mix of operational and analytical experience?
- What is the proposed team's mix of consultants and full-time members?
- How do you train your full-time team members? How do you train your consultants?
- Does a conflict of interest exist between your team and my program? How do you know?
- Can your organization work with members of my program? With foreign nationals?
- Can you fix problems your assessment identifies?
- Do you have domain experts needed to assess my program?
- What is your operational authority: military, Congressional, etc.?
- What facilities do you have that are needed to assess my program?
- What is your capacity? Can you field multiple red teams at the same time? Can you maintain a single red team for the duration of my program?

Knowledge

- Why is red teaming of value to my program?
- How is my program similar to programs you have red teamed before?
- Is there more than one way to red team? How?
- How should I apply red teaming to my program?
- How would you compose a team and apply it to the problem at hand?
- How can your results be reproduced by your team or another team?
- Where in the lifecycle should a system be red teamed?
- Can you cite an example system you have red teamed?
- How much should I spend on red teaming? Is it a good return on my investment?
- How are you contributing to the red teaming community (body of knowledge)?
- How do you maintain currency in knowledge, skills, and methods?

4 Plan to use your red team deliverables

Use *behavioral narratives* to ...

- Verify red team analysis
- Replay red team actions, possibly under different conditions
- Train responders by replaying red team actions

Use *attack graphs* or *trees* to ...

- Identify points of mitigation
- Explore new or incrementally different scenarios
- Anticipate adversary goals by observing prior behavior

Use *attack tools* to ...

- Validate attack plans and verify that identified vulnerabilities are exploitable
- Regression test future system iterations

Use *adversary models* to ...

- Explore new or incrementally different scenarios
- Train additional red teams to behave as a given adversary, or blue teams to recognize an adversary by its behavior
- Prune attack paths

Use *attack plans* to ...

- Support further red team activities, including red team games and opposing force activities
- Replay an attack to test proposed remediation
- Regression test future system iterations

Use *measures* and *metrics* to ...

- Measure progress toward program goals
- Decide whether to proceed to next program phase
- Report progress toward program goals

Sandia National Laboratories Information Design Assurance Red Team™
http://idart.sandia.gov | idart@sandia.gov | SAND2017-9535 TR
Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

IDART Information Design Assurance Red Team