Testing Standards and Methods for the DOD Cyber Range Infrastructure

March 26, 2019

This briefing transmits preliminary results of RAND research.
It has not been formally reviewed or edited & has not been cleared for public release.
Contents of this briefing should not be cited or quoted without permission of the authors.

Outline

- Overview of RAND research:
  - Phase 1: Analysis of cyber test range needs
  - Phase 2: Compilation of cyber test range tools and methods
  - Phase 3: Standardized tool taxonomy and standardized methodologies
- Cyber Range Interoperability Standards Working Group

RAND Research Phase 1: Cyber Test Needs

- Needs were developed from site visits, stakeholder interviews, document reviews, use cases, and review of DOT&E reports
  - "Needs" capture capabilities necessary to conduct cyber tests, but not intended to reflect validated requirements in the formal DoD sense
- 71 unique needs were identified
- Of these, 10 needs were found to be potentially highly impactful
  - Highest potential impact related to the need to expand and retain the pool of trained cyber personnel
- Results were compared with high priority needs identified by Cyber Test Range Requirements Working Group (CTRRWG)
  - CTRRWG did not include personnel
  - 5 other needs were common between the two approaches

RAND/CTRRWG Shared High Impact Needs

- **Modeling and Simulation**: Develop and provide the ability to model the effects of cyber attacks on the system and the missions it is used to conduct, enabling evaluation of the system's resiliency to attack and the risks to mission success if attacks succeed.
- **Accreditation Policy**: Establish policy setting cross-DoD standards for accrediting and using red teams that are not accredited and certified by the NSA.
- **Scheduling of Range Resources**: Establish central database of plans and schedules for conducting cyber test events on all cyber ranges.
- **Traffic Generation**: Develop or acquire and make widely available in a central repository tools capable of generating realistic traffic on networks using both IP-based and non-IP-based protocols.
- **Malware Handling**: Develop policy and processes for cyber testing of full-up systems using replicating malware, including provisions required for isolating the systems under test to assure malware does not spread beyond agreed boundaries, as well as processes to sanitize systems after testing.

RAND Research Phase 2: Compilation of Tools and Methods

- Cyber testing tools
  - Types and characteristics of tools, protocols, processes, etc. that enable the creation of a standard “tool kit” for localized and distributed cyber testing
  - Not intended to dictate the tools and methods every cyber test uses, but to encourage a common baseline for evaluating the results of those tests
- Cyber testing methodologies
  - Approaches for designing statistically significant cyber tests and establishing, to the extent possible, the confidence that can be associated with cyber test results

RAND Research Phase 3: Standardized Methodologies

- Building on our previous research, RAND is exploring standards and methodologies for comprehensively testing DoD platforms
  - Consider the implication of these standards on the DoD cyber test range infrastructure
  - Identify various methodologies that are in use
  - Explore the relative strengths, weakness, and implicit assumptions of each
  - Explore the extent to which the implicit or explicit assumptions apply in the cyber world
  - Maintain flexibility to meet customer needs

RAND Research Phase 3: Standardized Taxonomies of Cyber Testing Tools

- A definitive taxonomy of cyber testing tools is needed
  - Tools often presented as suites of capabilities that cover variety of needs, complicating comparison across tools
  - Was discussed at the Cyber DT Cross-Service Working Group in August 2018
- Towards a cyber test tool taxonomy
  - Cyber Range Event Process categories (Jan 2015)
    - 8 testing tool categories
  - NCR Tool categories (Feb 2016)
    - The NCR's *Top 10 Lessons Learned* briefing identified 14 testing tool categories
  - Literature Review categories (FY18)
    - We identified 11 testing tool categories

Example of Cyber Testing Tool Categories Derived from Literature Review

- Log collect tools
- Penetration testing tools
- Data collection tools
- Visualization tools
- Sanitization tools
- Traffic generation tools
- Data analysis tools
- Virtualization tools
- Range buildout/ configuration tools
- Software analysis tools
- Planning and scheduling tools

RAND Research Phase 3: Cyber Testing Methodologies

- Compare and assess the cyber testing methodologies identified as part of Phase 2
  - Examine applicability to
    - Specific systems and scenarios
    - Range of systems and scenarios
- Explore the accuracy, precision, and confidence of cyber testing methods
- TRMC is examining ways to engage and energize community around the need for cyber test interoperability standards


RAND
CORPORATION

10 Significant Needs Identified in Phase I

Need #	Description
4	Test protocols/TEMPS should include early testing and operational testing to establish mission impact of realistic cyber attack -- ensure that infrastructure can fully represent and fully support realistic cyber testing (including "cyber live fire" testing).
5	Establish policy requiring as a first preference fully representative system test articles be made available for government cyber testing, with provisions established for restoring the systems used in testing if they are corrupted.
22	Develop and provide the ability to model the effects of cyber attacks on the system and the missions it is used to conduct, enabling evaluation of the system's resiliency to attack and the risks to mission success if attacks succeed.
26	Implement policy changes that expand the limited pool of trained personnel.
31	Develop an Intuitive, useable tool for designing virtual networks using a repository of completed designs.
43	Establish policy setting cross-DoD standards for accrediting and using red teams that are not accredited and certified by the NSA.
50	Establish central database of plans and schedules for conducting cyber test events on all cyber ranges.
53	Develop or acquire and make widely available in a central repository tools capable of generating realistic traffic on networks using both IP-based and non-IP-based protocols.
57	Provide network connectivity at the appropriate security level to support realistic cyber testing, including insider, near-sider, and outsider attacks, and enabling full participation of all entities involved in the testing in real time.
69	Refine policy and processes for cyber testing of full-up systems using malware, including provisions required for isolating the systems under test to assure malware does not spread beyond agreed boundaries, as well as processes to sanitize systems after testing.