Operationally Assessing Cyber Defenses

Allison Goodman

The Challenge: When Congress directed the Director, Operational Test and Evaluation to establish a Cybersecurity Assessment Program, DOT&E asked IDA to help plan realistic data-based cyber evaluation events during operational exercises, execute the events, and provide rigorous post-event analyses. Analytical methods for these evaluations must continue to evolve and become more rigorous as our cyber adversaries become more sophisticated.

DOT&E conducts data-based cyber evaluations during Combatant Command and Service-level exercises to... determine the effect of cyber activities on operational missions.

IDA supports the Director, Operational Test and Evaluation (DOT&E) on the congressionally mandated Cybersecurity Assessment Program. Through this program, DOT&E conducts data-based cyber evaluations during Combatant Command and Service exercises to understand how a cyber adversary can attack and compromise networks, characterize the defensive response, and determine the effect of cyber activities on operational missions. The program uses DoD Cyber Red Teams to portray a live, thinking, cyber adversary, who join with the traditional exercise Opposing Force to target critical Combatant Command Missions within the context of exercise scenarios designed to exercise operational plans. IDA analyses in support of DOT&E have produced recommendations for both local and department-wide defensive approaches and vulnerability mitigation strategies. This article describes how IDA supports the DOT&E Cybersecurity Assessment Program and the analytical methods used to conduct these data-based evaluations.

IDA support spans the lifecycle of the exercise: planning, execution, and post-assessment reporting. During the planning events, IDA researchers help scope the cyber component of the event while still ensuring that the cybersecurity assessment will not negatively affect the exercise training objectives.

During the exercise, the operational test agencies collect data on four main cybersecurity functional areas: Protect, Detect, Respond, and Recover (PDRR). Data collection focuses on both those executing the exercise mission (operators and cyber defenders) and the opposing force portrayal (Red Team). IDA researchers are on site during exercise execution, ensuring data accuracy and completeness, as well as maintaining situational awareness for the post-assessment analysis and reporting.

The collection of PDRR data in the context of the exercise allows IDA researchers the ability to focus on attack threads, defensive responses, and mission effects. Attack threads detail each step in an attack, starting from intrusion and ending at either mission effect or detection. Figure 1 shows the intended outcomes of two notional cyber-attacks, which will be used to illustrate the analytical process.

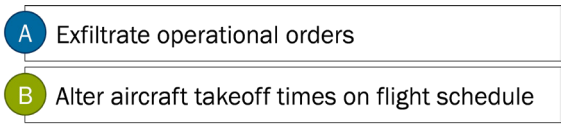

Figure 1. Notional Cyber Attack Thread Outcomes

Red Teams provide detailed information about each action taken during the exercise, including methods and tools used. IDA researchers organize these actions by those leading to the identified attack thread outcomes and map the progression of the cyber-attack from ingress to conclusion. Figure 2 shows the simple and notional Attack Thread A to illustrate this mapping. In this example, the Red Team affects the confidentiality of the operational orders by exfiltrating them from the system and network. Defenders did not detect the Red Team movement through the network or the exfiltration of data, and therefore do not appear in the notional thread.

Attack Thread B illustrates the combination of the Red Team actions with the cyber defender actions (Figure 3). In this example, the end user detected and reported the modified takeoff times, and the cyber defenders responded by identifying and blocking the originating IP address. Data for these cyber actions, detections, and response comes from multiple sources, which IDA researchers combine to present the end-to-end picture of each cyber-attack.

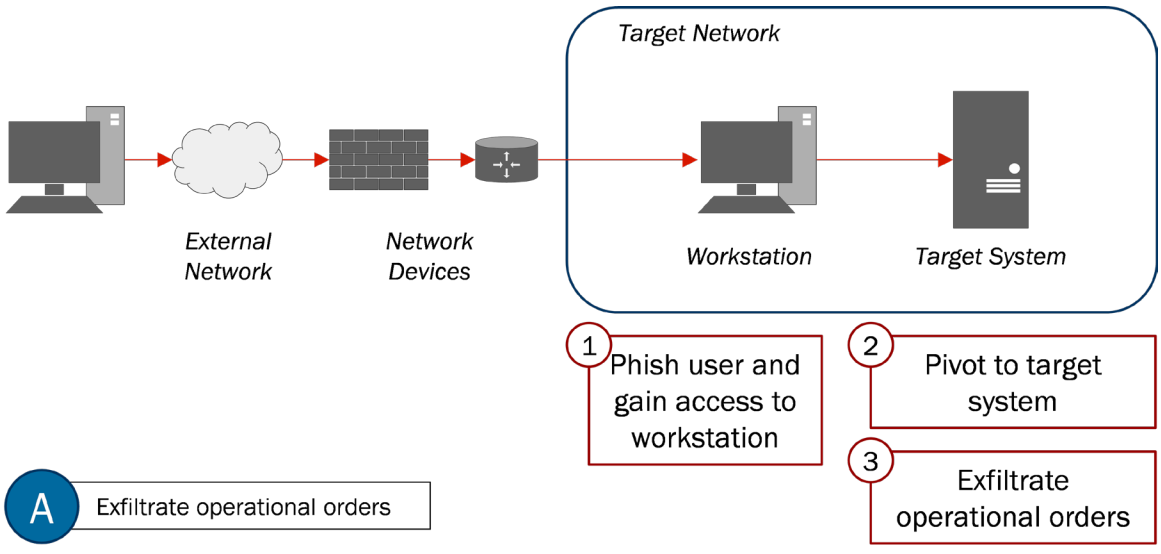

Figure 2. Notional Attack Thread A

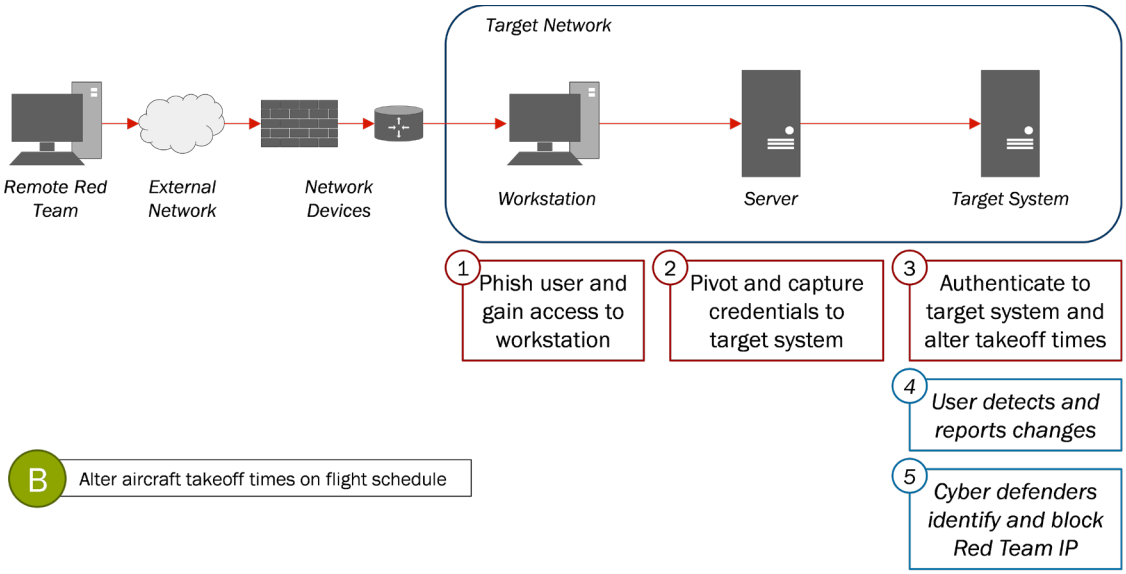

Figure 3. Notional Attack Thread B, including cyber defender actions

Next, IDA researchers incorporate the effect on the operational mission from the exercise scenario, providing context to the outcomes of each attack, as applicable. Following Attack Thread A, if the Red Team exfiltrates the operational orders after they were already executed, this has little effect on the overall mission. However, if the Red Team exfiltrates them prior to execution of the orders, the opposing force has knowledge of future friendly force activity, providing the opportunity to disrupt operations.

To provide further context, IDA researchers also determine the capability level required to execute each attack thread by evaluating the knowledge; tools, techniques, and procedures (TTPs); and planning required to execute each attack thread. The capability is rated on a four-level scale ranging from nascent to advanced for each of these categories and their sub-categories. Table 1 shows the criteria for each capability rating by categories. The circles indicate the notional capability breakdown for Attack Threads A and B. The level of capability required to achieve a particular attack thread is then the greatest capability level required across all categories. Therefore, Attack Thread A required Limited capability to achieve and Attack Thread B required Moderate capability to achieve.

These analyses provide Combatant Commands and the Services with not only an analysis of network vulnerabilities, but also the potential effects that vulnerabilities could have on their missions and the capabilities required to achieve those effects.

Table 1. Notional Capability Required to Complete Attack Threads A and B

		Nascent	Limited	Moderate	Advanced
Knowledge	General Systems	Common OS (Windows client, Linux), and software applications (Adobe, Oracle), consumer-market hardware (PCs, home routers), common network and data protocols (IP, Ethernet, 802.11), general-purpose languages (Python, Java, SQL), common OS-specific languages (Unix shell, PowerShell), public cryptography and standard authentication (PGP, NTLMv2, Kerberos) B	Commercial enterprise OS (MS Server, virtualization environments), industry market network OS (Cisco IOS, Juniper) and devices (routers, proxies, VPN), defensive devices (IDS, firewalls), cellular data protocols (GSM, 4G LTE), common firmware (BIOS), common architecture assemblers (Intel, ARM, MIPS), token-based authentication (CAC, ActiveID) A	Common military software (GCCS, HBBS, TBMCS), less-common network and data protocols (tactical data links, radio, CAN bus, other MIL-STD interfaces), embedded systems (PLCs, digital signal processors) and software (embedded C, RTOS), specialized firmware (fuzes, avionics), server/ military assemblers (SPARC, MIL-STD 1750A), biometric-based authentication	Restricted and highly classified military systems, software, and weapons platforms, classified cryptography (NSA Type 1) and associated hardware (TACLANE), cross-domain devices (Radiant Mercury, ISSE Guard)
	Target Network and Systems	Information about target environment found from commonly available open sources (commercial Internet, literature) or from external reconnaissance of target network and systems	Knowledge of network and system specifications (individual user account information, hostnames, IP address of few systems) and type/configuration of host-based defenses equivalent to an authorized user in the target environment A B	Knowledge of network and system specifications (configuration settings, software inventories) and type/configuration of networked defenses (IDS, ACLs) equivalent to an authorized Administrator in the target environment	Knowledge of network and system specifications (network architecture, Domain-wide configurations and user account information) and defenses (full defense in depth) equivalent to an authorized Domain Administrator in the target environment
	Target Operations	Information found from commonly available open sources or from external reconnaissance of target organization	Knowledge from more specialized literature or equivalent to prior experience with target operations, including key information or supporting systems A	Knowledge equivalent to substantial prior experience with target operations, including work flow and sub-task objectives B	Knowledge of current target operations equivalent to an experienced authorized operator
Tools	Software and Hardware	Freeware (Kali, Scapy, Poison Ivy) and inexpensive commercial tools (Retina, Cobalt Strike), public exploits of known vulnerabilities (Metasploit, w3af), inexpensive hardware (PCs, Yellowjacket, rogue WAPs like PWN Plugs, physical access tools, connectors) A	Commercial software (Core Impact, Metasploit Pro), 0-day exploits of less common/more vulnerable software (Adobe, MAC OSX), custom software (kernel rootkits, C2 agents) and hardware (GPU clusters, covert rogue WAPs) costing $10,000s or dozens of man-hours B	0-day exploits of more common/less vulnerable software (Windows, iOS), custom software (polymorphic malware, covert remote access tools and loggers, boot sector/firmware rootkits, forged SSL certificates) and hardware (rogue MIL-STD WAPs) costing $100,000s or hundreds of man-hours	0-day exploits of restricted military systems and industrial control systems, custom software (firmware-resident malware, high-level programming languages) and custom hardware (covert RF WAPs, chipset backdoors, TEMPEST devices), costing $1,000,000s or thousands of man-hours
Operations	TTPs	No demonstrated stealth, non-attribution or efficient use of resources A B	Low degree of stealth (C2 over uncommon protocols, changing signatures or running tools in memory to avoid common A/V, rootkits), non-attribution (log purging, IP/MAC spoofing, TOR), or efficiency in use of resources consistent with intent	Some degree of stealth (C2 with custom encoding, disabling A/V or IDS), non-attribution (code obfuscation, fast-fluxing), or efficiency in use of resources consistent with intent	High degree of stealth (strategic onetime use C2, full control of defensive infrastructure), non-attribution (false flag operations), or efficiency in use of resources consistent with intent
	Planning	Opportunistic actions, no planning	Intent and short-range plans formed on-the- fly as needed A B	Organizes (one or more) operations with specific target systems and associated effects on target organization	Organizes multiple operations against separate targets, synchronizing timing, accesses, and planned second-order effects

IDA continually evolves this methodology as the cyber-attacks and defenses grow in complexity. IDA researchers identify data gaps and ensure that upcoming assessments fill those gaps. Each exercise presents the opportunity to research new questions and provide more insight into the state of cybersecurity across DoD.

Dr. Allison Goodman is a Research Staff Member in IDA's Operational Evaluation Division. She holds a Doctor of Philosophy in biomedical engineering from Virginia Polytechnic Institute and State University.