INTRODUCTION TO RED TEAMING

CYBERSECURITY TRAINING SIMPLIFIED

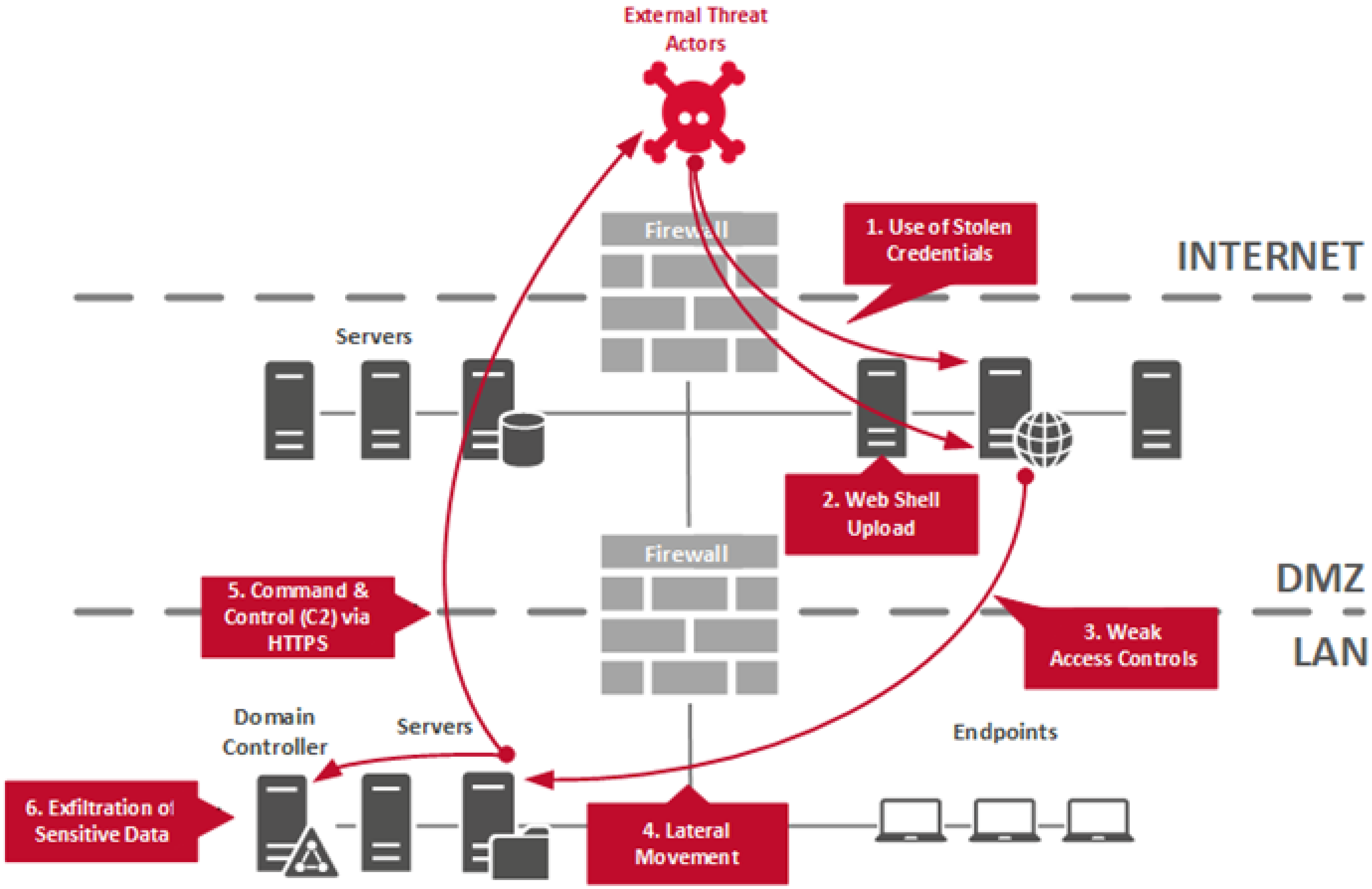
HACKERSPLOIT.ORG // HACKERSPLOIT.ACADEMY

$HACKERSPLOIT_

WHAT IS RED TEAMING?

- Red Teaming is the process of emulating the Tactics, Techniques & Procedures (TTPs) of real-world threats/APT groups with the goal of measuring the effectiveness and resilience of defenders (Blue Team), employees, processes and the underlying technology of a target organization.
- The underlying goal/motive of Red Teaming is to get a better, more holistic understanding of an organization's ability to detect and defend against adversarial TTPs.
- Red Teaming is a practice that was adopted from the military, whereby military units are tasked to operate as adversaries and are required to simulate attack techniques utilized by adversaries in order to assess the abilities of the defending team.
- This process provides an organization with valuable information on their blue team's abilities and outlines where detection and defense controls/mechanisms can be improved.

WHAT IS RED TEAMING?

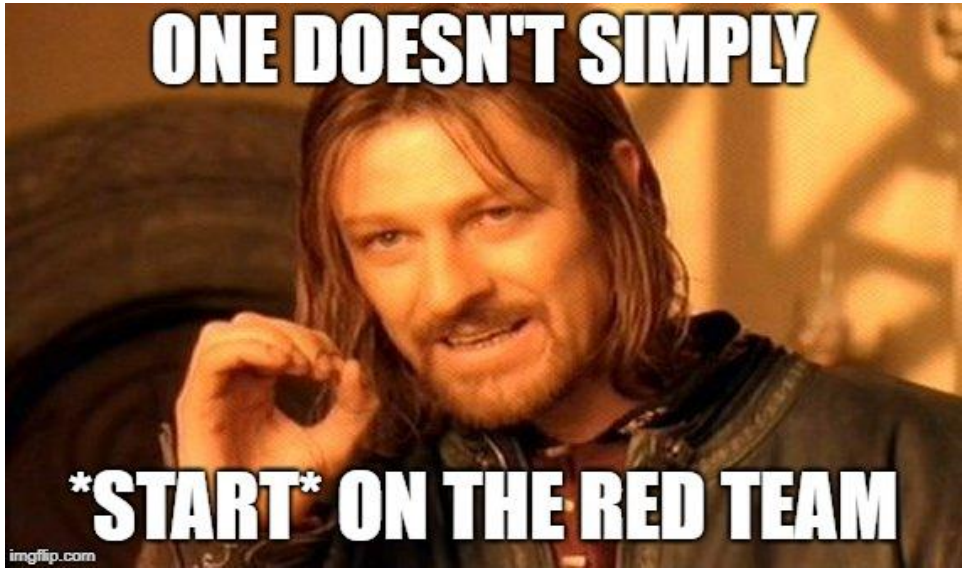


WHAT IS RED TEAMING?

- Given the perceived nature and scope of a Red Team operation, it is typically misconstrued as an unplanned, unorganized ad-hoc pentest. However, this couldn't be farther from the truth.

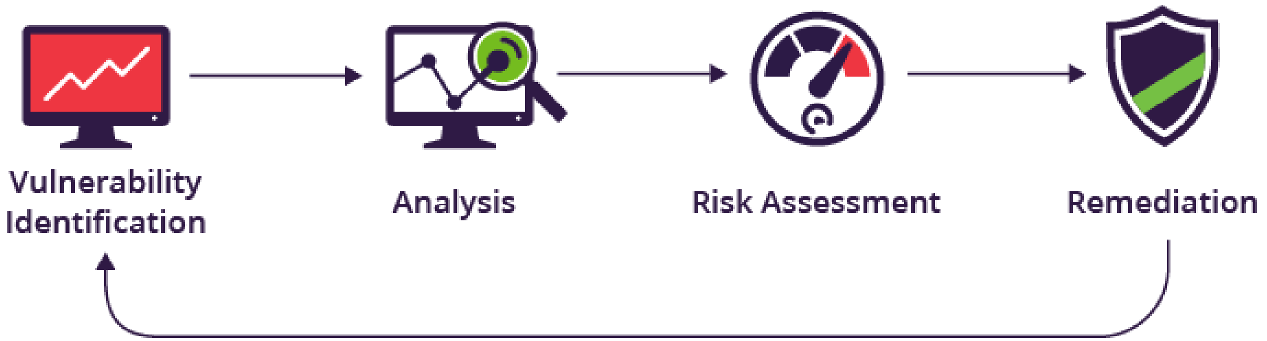
SECURITY ASSESSMENTS

- In order to understand the importance of Red Teaming, you need to understand the various types of security assessments commonly used by organizations, what their objectives are and how they differ.
- From an offensive perspective, organizations have typically used various security assessments to get an understanding of their current threat surface, risk, potential business impact and defense capabilities.



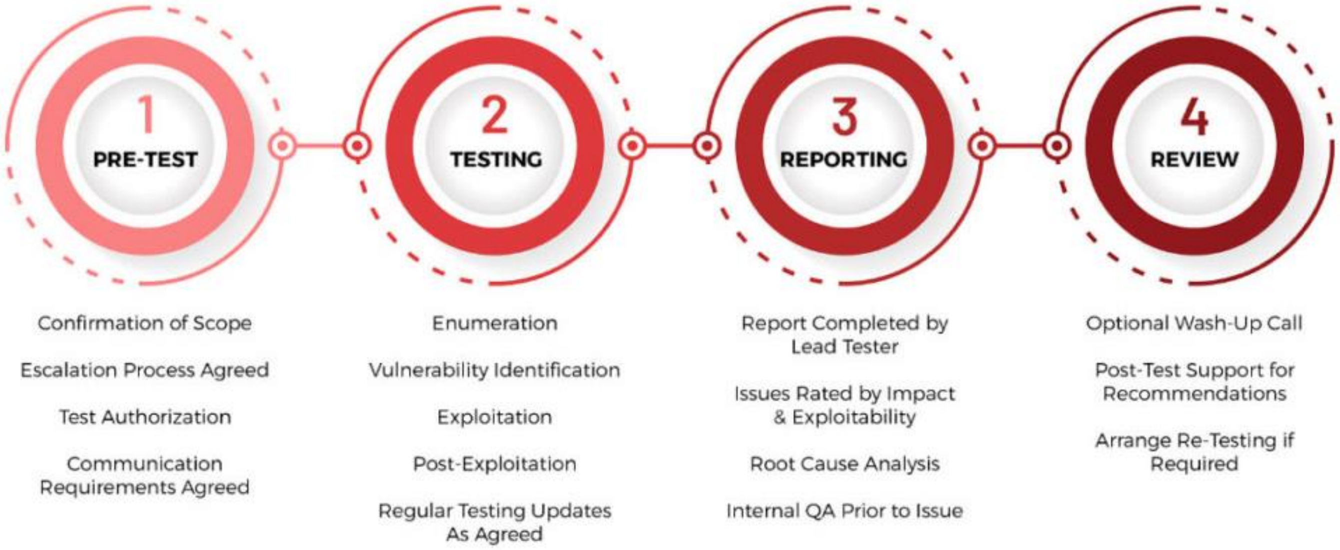
VULNERABILITY ASSESSMENTS

- Vulnerability assessments are the most common form of preventative security; the primary objective is to scan all workstations and digital assets in order to identify vulnerabilities and misconfigurations. This provides an organization with a clearer picture of their threat surface and security posture.
- This information helps a company determine where they should focus their patching and remediation efforts.
- Vulnerability assessments are very useful in reducing the attack surface but fall short in extrapolating the organizational risk of identified vulnerabilities.



PENETRATION TESTING

- Penetration Testing is the process of identifying and attempting to exploit vulnerabilities on target systems. Penetration tests improve on vulnerability assessments by verifying the potential impact of a vulnerability by attempting to exploit said vulnerability.
- Penetration testing also goes beyond initial access (exploitation) and involves performing various post-exploitation activity.



1 PRE-TEST

- Confirmation of Scope
- Escalation Process Agreed
- Test Authorization
- Communication Requirements Agreed

2 TESTING

- Enumeration
- Vulnerability Identification
- Exploitation
- Post-Exploitation
- Regular Testing Updates As Agreed

3 REPORTING

- Report Completed by Lead Tester
- Issues Rated by Impact & Exploitability
- Root Cause Analysis
- Internal QA Prior to Issue

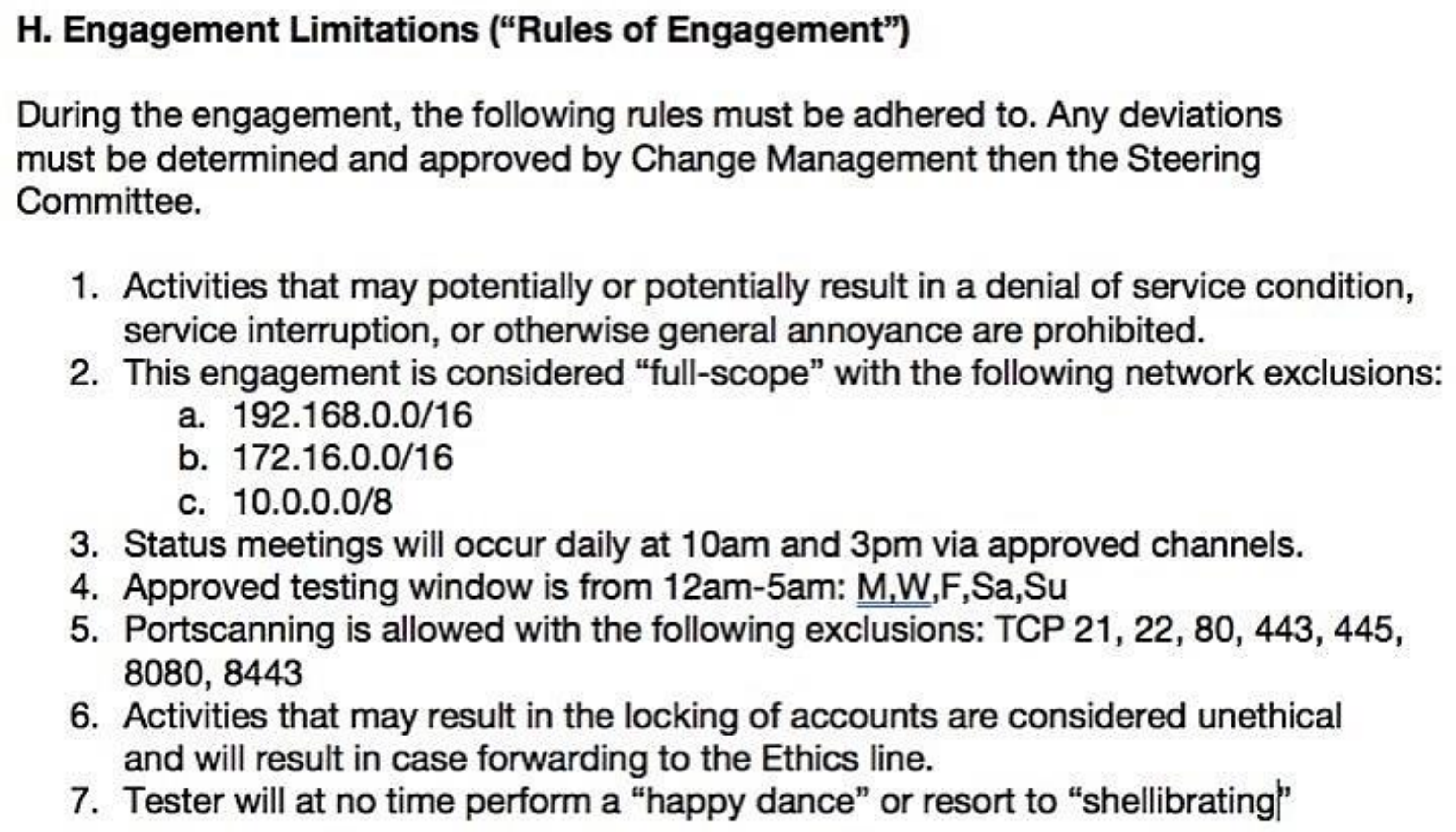
4 REVIEW

- Optional Wash-Up Call
- Post-Test Support for Recommendations
- Arrange Re-Testing if Required

PENETRATION TESTING

- The primary objective of a penetration test is to identify and exploit vulnerabilities in target systems in order to measure the risk associated with the exploitation of the target's attack surface.
- Penetration Tests provide an organization with a much more accurate understanding of how a potential threat could gain access to their environment and provides valuable information on where detection and defense capabilities need to be improved.
- Penetration tests are quite limited with regards to their ability to emulate/simulate a real threat actor primarily because of the scope. Penetration tests can be either black-box or white box and can be very loud.
- Given that the goal of a penetration test is to identify and exploit vulnerabilities in target systems, risk is typically measured and is limited to the workstations/assets within the pre-defined scope and does not encompass employees, defenders and processes.

PENETRATION TESTING – ROE EXAMPLE



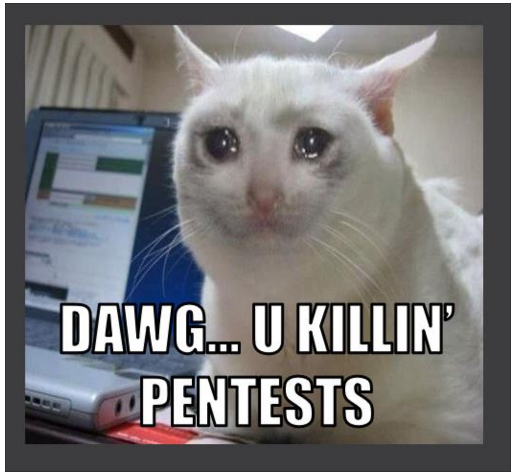
H. Engagement Limitations (“Rules of Engagement”)

During the engagement, the following rules must be adhered to. Any deviations must be determined and approved by Change Management then the Steering Committee.

1. Activities that may potentially or potentially result in a denial of service condition, service interruption, or otherwise general annoyance are prohibited.
2. This engagement is considered “full-scope” with the following network exclusions:
    a. 192.168.0.0/16
    b. 172.16.0.0/16
    c. 10.0.0.0/8
3. Status meetings will occur daily at 10am and 3pm via approved channels.
4. Approved testing window is from 12am-5am: M,W,F,Sa,Su
5. Portscanning is allowed with the following exclusions: TCP 21, 22, 80, 443, 445, 8080, 8443
6. Activities that may result in the locking of accounts are considered unethical and will result in case forwarding to the Ethics line.
7. Tester will at no time perform a “happy dance” or resort to “shellibrating”

LIMITATIONS OF PENETRATION TESTS

- Given the underlying objective, penetration testers usually do not have to worry about tripping alerts or evading detection. As a result, penetration testers are typically noisy and loud. Real-world threats are not.
- A traditional penetration test is likely to ignore attack vectors like social engineering and physical intrusions. (Very common with real adversaries).
- Penetration Testers must abide by strict Rules of Engagement and the predefined scope.
- In certain cases, the organization may whitelist the penetration tester's attack infrastructure and in certain cases, defense and detection mechanisms may be relaxed.



WHY RED TEAM?

- Red Teaming allows you to assess and measure the effectiveness and resilience of employees, defenders and processes used to defend a company's digital infrastructure.
- Very useful for measuring the Blue Team's ability to detect and defend against adversaries.
- Used to train the Blue Team. Defenders require frequent training and practice in order to be effective.
- Exposure to real-world threats/APTs and their corresponding TTPs, tradecraft and malware.

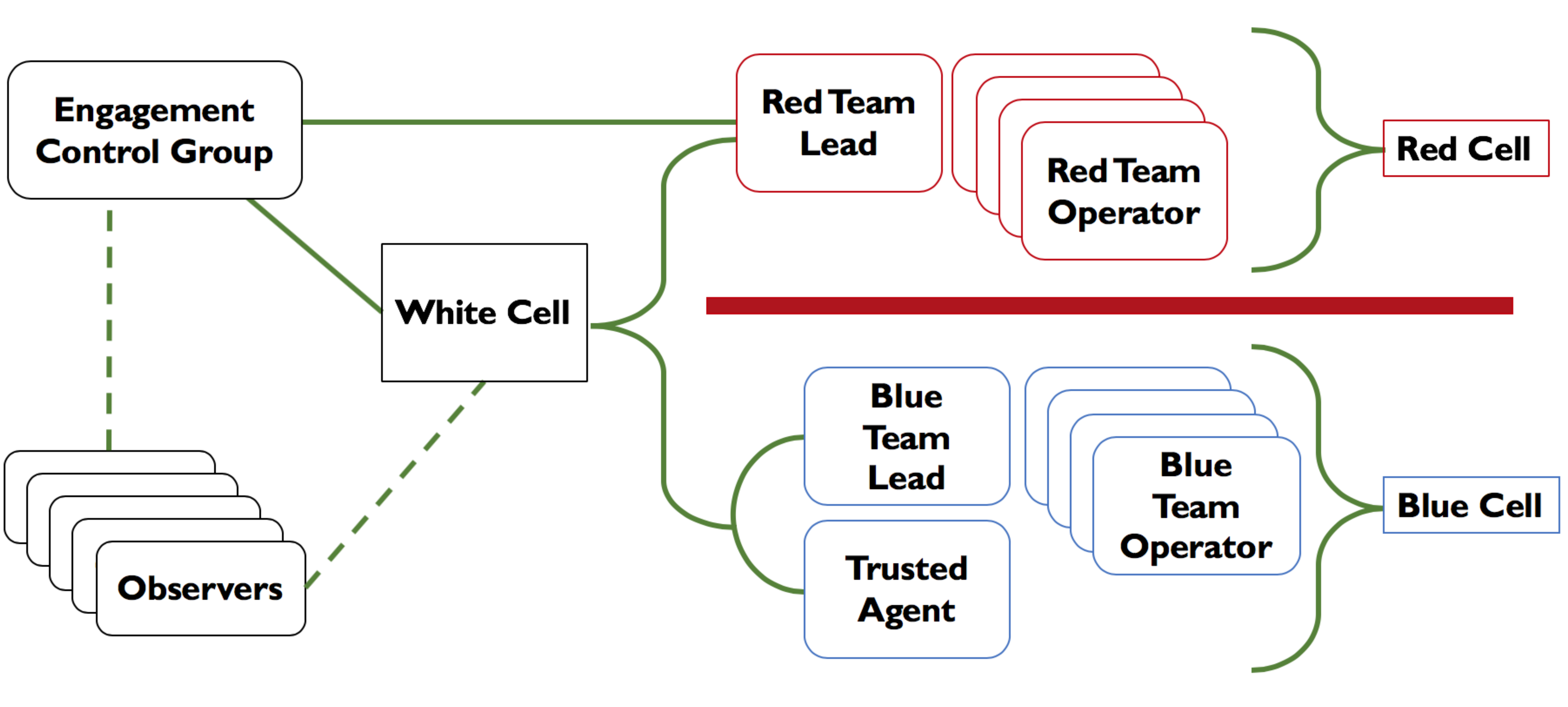
ESSENTIAL TERMINOLOGY

TERM	DEFINITION
TTPs	Tactics, Techniques & Procedures.
Tradecraft	Techniques and procedures during an attack campaign.
OPLOG	Operator logs are the records generated by Red Team operators during an engagement. These logs have specific and required fields that must be captured.
C2	Command and Control
Exfiltration	Process of extraction of information/data from a target system through a covert channel.
IoC	Indicator of compromise – Artifacts used to identify adversarial activity.
OPSEC	Operational Security – What the Blue Team can observe and is used to minimize exposure.
Operational Impact	Effect of an objective driven action within a target environment.
Situational Awareness	Phase of a Red Team operation used to gather information on targets and the target environment. This information used to determine the next action.
CTI	Cyber Threat Intelligence – Information collected, aggregated, analyzed and interpreted to provide the context for decision-making processes regarding threats.

TYPES OF RED TEAM ENGAGEMENTS

ENGAGEMENT	USE CASE/DEFINITION
Full Simulation	Simulates a threat/adversary’s attack flow.
Adversary Emulation	Emulating/Mimicking an adversary’s/APT’s TTPs with little or no deviation.
Assumed Breach	The Assumed Breach Model assumes a threat has some level of access to a target at the initiation of the engagement.
Table-top Exercise	An over the table simulation where scenarios are discussed between the red and blue teams to evaluate how they would theoretically respond to certain threats.

RED TEAM ROLES AND RESPONSIBILITIES



RED TEAM ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Red Cell	Group that plays OPFOR (opposing force) during red vs. blue exercises. A red cell is the components that make up the offensive portion of a red team engagement that simulates the strategic and tactical responses of a given target. The red cell is typically comprised of red team leads and operators and is commonly referred to as Red Team instead of Red Cell.
Blue Cell	The blue cell is the opposite side of red. Is it all the components defending a target network. The blue cell is typically comprised of blue team members, defenders, internal staff, and an organization's management.
White Cell	Serves as referee between Red Team activities and defender responses during an engagement. Controls the engagement environment/network. Monitors adherence to the ROE.

RED TEAM ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Red Team Lead	Serves as the operational and administrative lead for the Red Team. Conducts engagement, budget, and resource management for the Red Team, Provides oversight and guidance for engagements, capabilities, and technologies. Ensures adherence to all laws, regulations, policies, and Rules of Engagement.
Red Team Assistant Lead	Assists the team lead in overseeing engagement operations and operators. Can also assist in writing engagement plans and documentation if needed.
Red Team Operator	Complies with all Red Team requirements under the direction of the Red Team Lead. Operational executor of the engagement. Applies Red Team TTPs to the engagement. Provides technical research and capability to the Red Team. Keeps detailed logs during each phase of the engagement.

Thank You