# PLANNING RED TEAM ENGAGEMENTS

# SCOPE & OBJECTIVES

- Defining Red Team engagement goals can be difficult and tedious primarily because there needs to be a synthesis between the Red Team and the client.
- This is especially true for organizations new to Red Teaming. Whether you are on the delivery or receiving end of a Red Team engagement, the solid goals must be decided to have successful Red Team engagement.
- When analyzing a client's desired objectives, one key factor to consider is the depth and nature of the engagement.
- Red Team engagements can be categorized in to:
  - Full Simulation/Extended Pentest
  - Adversary Emulation

# SCOPE & OBJECTIVES

- The type of engagement to utilize and the corresponding methodology used will heavily depend on the objectives defined by the client.
- Once objectives have been defined, engagement plans will need to be setup to further expand on the specifics of the engagement.
- Another key factor to consider is the engagement scope, the scope of an engagement will depend on the target infrastructure.
- The scope outlines what you can or cannot target and what you can or cannot do on target systems.
- The scope is always defined by the client and should be strictly adhered to.

# EXAMPLE OF OBJECTIVE(S)

- Identify system misconfigurations and network weaknesses.
  - Focus on external, public-facing systems.
- Determine the effectiveness of endpoint detection and response systems.
- Evaluate overall security posture and response.
  - SIEM and detection measures.
  - Remediation.
  - Segmentation of DMZ and internal servers.
- Evaluate the impact of data exposure and exfiltration.

# RULES OF ENGAGEMENT (ROE)

- The Rules of Engagement establish the responsibility, relationship, and guidelines between the Red Team, the network owner, the system owner, and any stakeholders required for engagement execution.

- The ROE documents the target information, approvals, threat implementation, activities, and issues required to staff, coordinate, and execute engagements within the target environment.

# RULES OF ENGAGEMENT (ROE)

- Rules of Engagement (ROE) is a document that outlines the scope and objectives of the engagement.
- Rules of Engagement establish the responsibility, relationship, and guidelines between the Red Team, the network owner, the system owner, and any stakeholders required for engagement execution.
- The ROE documents the target information, approvals, threat implementation, activities, and issues required to staff, coordinate, and execute engagements within the target environment.

# RULES OF ENGAGEMENT (ROE)

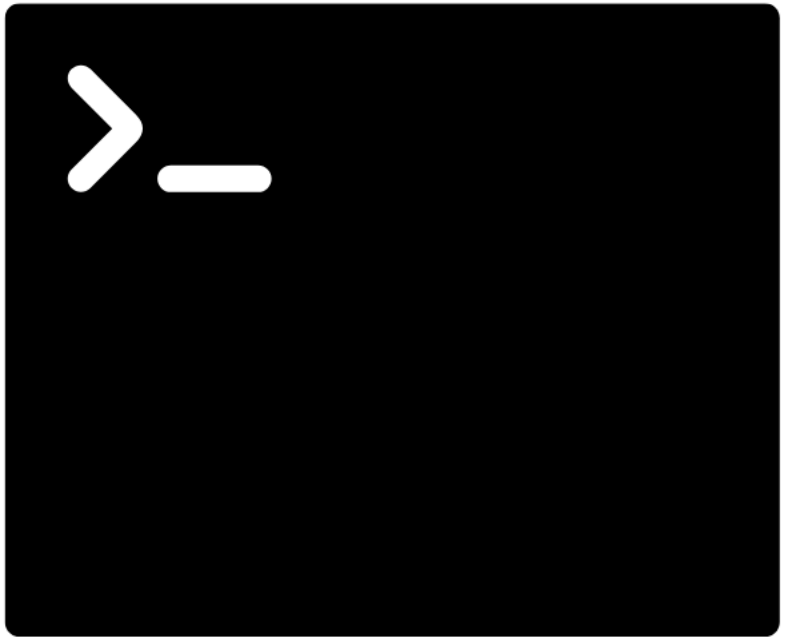
- The body of the ROE document should have the following information:
  - The methodology being used or the methodology that was followed.
  - A high-level description of the types of activities that may be executed.
  - The types of hardware and software that may be employed.
  - A recommended deconfliction process
  - Roles and responsibilities of each functional group.
  - The identification of and references to appropriate legal requirements (PCI, FERPA, HIPAA, HITEC, SOX, GLBA, etc.).
  - A legal responsibility disclaimer (federally mandated requirements for the Red Team to report certain findings).

# PLANNING RED TEAM OPERATIONS

- Planning a Red Team engagement can be difficult. This is especially true for organizations new to Red Teaming. Whether you are on the delivery or receiving end of a Red Team engagement, a solid plan must be laid out to have successful Red Team engagement.
- Red Team engagement planning can be broken down in to 4 primary types.

| PLAN | DEFINITION |
|---|---|
| Engagement Plan | Outlines the technical requirements of the Red Team. (CONOPS, Resource Requirements & Timelines) |
| Operations Plan | Detailed version of the engagement plan. (Roles & responsibilities, operators) |
| Mission Plan | Execution plan (Commands to run, when to execute them, responsible operator) |
| Remediation Plan | Outlines the next phase of the engagement once the operation is done (Reporting and remediation) |

# Practical Demo



RED TEAM ROE & REPORT

# Thank You

CYBERSECURITY TRAINING SIMPLIFIED

HACKERSPLOIT.ORG // HACKERSPLOIT.ACADEMY

$HACKERSPLOIT_