Red Team Engagements

Introduction

The key to a successful engagement is well-coordinated planning and communication through all parties involved. This room will focus on various components of a red team engagement and planning and documenting a campaign for a red team engagement.

Red team engagements come in many varieties; including,

- Tabletop exercises
- Adversary emulation
- Physical assessment

Learning Objectives

- Understand components and functions of a red team engagement.
- Learn how to properly plan an engagement based on needs and resources available and TTPs.
- Understand how to write engagement documentation in accordance with client objectives.

Defining Scope and Objectives

Engagements can be very complex and bureaucratic. The key to a successful engagement is clearly defined client objectives or goals. Client objectives should be discussed between the client and red team to create a mutual understanding between both parties of what is expected and provided. Set objectives are the basis for the rest of the engagement documentation and planning.

Without clear and concrete objectives and expectations, you are preparing for a very unstructured and unplanned campaign. Objectives set the tone for the rest of the engagement.

When assessing a client's objectives and planning the engagement details, you will often need to decide how focused the assessment is.

Engagements can be categorized between a general internal/network penetration test or a focused adversary emulation. A focused adversary emulation will define a specific APT or group to emulate within an engagement. This will typically be determined based on groups that target the company's particular industries, i.e., finance institutions and

APT38. An internal or network penetration test will follow a similar structure but will often be less focused and use more standard TTPs.

The specifics of the approach will depend on a case-by-case basis of the engagement defined by the client objectives.

Client objectives will also affect the engagement's general rules of engagement and scope.

These topics will be expanded upon in Task 6.

The client objectives only set a basic definition of the client's goals of the engagement. The specific engagement plans will expand upon the client objectives and determine the specifics of the engagement. Engagement plans will be covered later within this room.

The next keystone to a precise and transparent engagement is a well-defined scope. The scope of an engagement will vary by organization and what their infrastructure and posture look like. A client's scope will typically define what you cannot do or target; it can also include what you can do or target. While client objectives can be discussed and determined along with the providing team, a scope should only be set by the client. In some cases the red team may discuss a grievance of the scope if it affects an engagement. They should have a clear understanding of their network and the implications of an assessment. The specifics of the scope and the wording will always look different, below is an example of what verbiage may look like within a client's scope.

- No exfiltration of data.
- Production servers are off-limits.
- 10.0.3.8/18 is out of scope.
- 10.0.0.8/20 is in scope.
- System downtime is not permitted under any circumstances.
- Exfiltration of PII is prohibited.

When analyzing a client's objectives or scopes from a red team perspective, it is essential to understand the more profound meaning and implications. When analyzing, you should always have a dynamic understanding of how your team would approach the problems/objectives. If needed, you should write your engagement plans or start them from only a bare reading of the client objectives and scope.
****

Answer the questions below:

Below is an example of the client objectives of a mature organization with a strong security posture.
Example 1 - Global Enterprises:

Objectives:

1. *Identify system misconfigurations and network weaknesses.*
    - *Focus on exterior systems.*
2. *Determine the effectiveness of endpoint detection and response systems.*
3. *Evaluate overall security posture and response.*
    - *SIEM and detection measures.*
    - *Remediation.*
    - *Segmentation of DMZ and internal servers.*
4. *Use of white cards is permitted depending on downtime and length.*
5. *Evaluate the impact of data exposure and exfiltration.*

Scope:

1. *System downtime is not permitted under any circumstances.*
    - *Any form of DDoS or DoS is prohibited.*
    - *Use of any harmful malware is prohibited; this includes ransomware and other variations.*
2. *Exfiltration of PII is prohibited. Use arbitrary exfiltration data.*
3. *Attacks against systems within 10.0.4.0/22 are permitted.*
4. *Attacks against systems within 10.0.12.0/22 are prohibited.*
5. *Bean Enterprises will closely monitor interactions with the DMZ and critical/production systems.*
    - *Any interaction with "*.bethechange.xyz" is prohibited.*
    - *All interaction with "*.globalenterprises.thm" is permitted.*

What CIDR range is permitted to be attacked?
Answer: 10.0.4.0/22

Is the use of white cards permitted? (Y/N)
Answer: Y

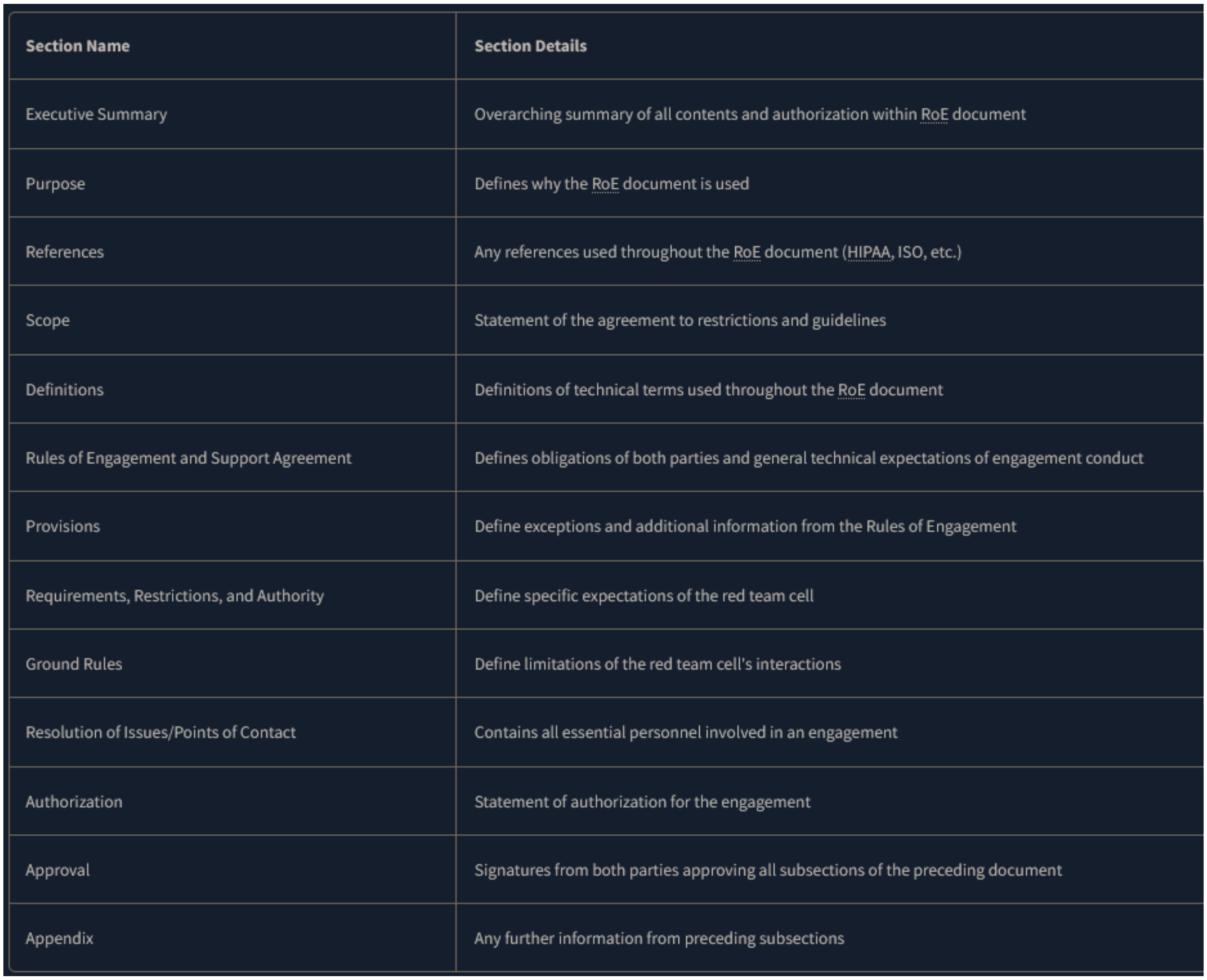
Are you permitted to access "*.bethechange.xyz?" (Y/N)
Answer: N
****

Rules of Engagement

Rules of Engagement (RoE) are a legally binding outline of the client objectives and scope with further details of engagement expectations between both parties. This is the first "official" document in the engagement planning process and requires proper authorization between the client and the red team. This document often acts as the general contract between the two parties; an external contract or other NDAs (Non-Disclosure Agreement) can also be used.

The format and wording of the RoE are critical since it is a legally binding contract and sets clear expectations.

Each RoE structure will be determined by the client and red team and can vary in content length and overall sections. Below is a brief table of standard sections you may see contained in the RoE.



Section Name	Section Details
Executive Summary	Overarching summary of all contents and authorization within RoE document
Purpose	Defines why the RoE document is used
References	Any references used throughout the RoE document (HIPAA, ISO, etc.)
Scope	Statement of the agreement to restrictions and guidelines
Definitions	Definitions of technical terms used throughout the RoE document
Rules of Engagement and Support Agreement	Defines obligations of both parties and general technical expectations of engagement conduct
Provisions	Define exceptions and additional information from the Rules of Engagement
Requirements, Restrictions, and Authority	Define specific expectations of the red team cell
Ground Rules	Define limitations of the red team cell's interactions
Resolution of Issues/Points of Contact	Contains all essential personnel involved in an engagement
Authorization	Statement of authorization for the engagement
Approval	Signatures from both parties approving all subsections of the preceding document
Appendix	Any further information from preceding subsections

When analyzing the document, it is important to remember that it is only a summary, and its purpose is to be a legal document. Future and more in-depth planning are required to expand upon the RoE and client objectives.

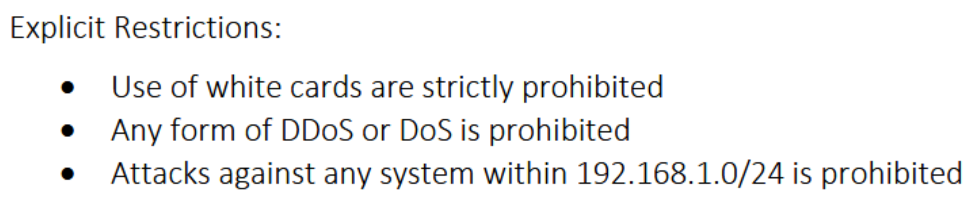
For this task we will use a shortened document adapted from redteam.guide.
****

Answer the questions below:

Download the sample rules of engagement from the task files.

Once downloaded, read the sample document and answer the questions below.
No Answer Needed

How many explicit restrictions are specified?

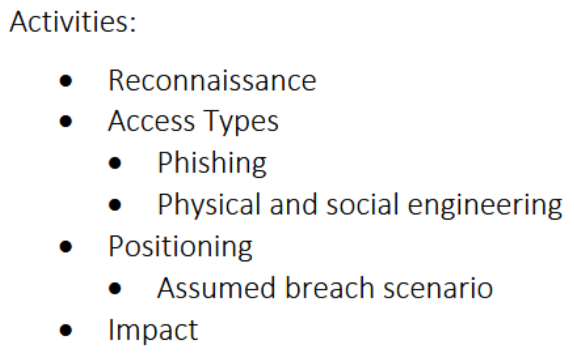


Explicit Restrictions:

- Use of white cards are strictly prohibited
- Any form of DDoS or DoS is prohibited
- Attacks against any system within 192.168.1.0/24 is prohibited

Answer: 3

What is the first access type mentioned in the document?



Activities:

- Reconnaissance
- Access Types
  - Phishing
  - Physical and social engineering
- Positioning
  - Assumed breach scenario
- Impact

Answer: Phishing

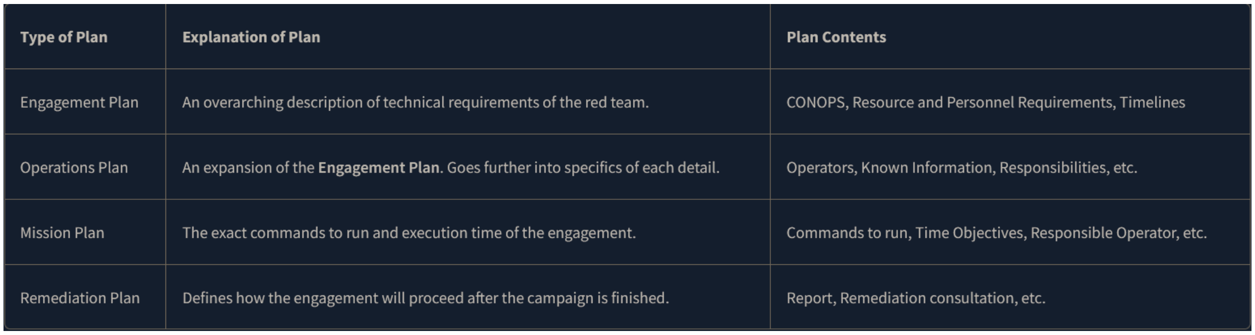
Is the red team permitted to attack 192.168.1.0/24? (Y/N)
That subnet is explicitly restricted.
Answer: N

****

Campaign Planning

Prior to this task, we have primarily focused on engagement planning and documentation from the business perspective. Campaign planning uses the information acquired and planned from the client objectives and RoE and applies it to various plans and documents to identify how and what the red team will do.

Each internal red team will have its methodology and documentation for campaign planning. We will be showing one in-depth set of plans that allows for precise communication and detailed documentation. The campaign summary we will be using consists of four different plans varying in-depth and coverage adapted from military operations documents. Each plan can be found in the table below with a brief explanation.



Type of Plan	Explanation of Plan	Plan Contents
Engagement Plan	An overarching description of technical requirements of the red team.	CONOPS, Resource and Personnel Requirements, Timelines
Operations Plan	An expansion of the **Engagement Plan**. Goes further into specifics of each detail.	Operators, Known Information, Responsibilities, etc.
Mission Plan	The exact commands to run and execution time of the engagement.	Commands to run, Time Objectives, Responsible Operator, etc.
Remediation Plan	Defines how the engagement will proceed after the campaign is finished.	Report, Remediation consultation, etc.

Another example of a campaign plan is the redteam.guide engagement checklist. The checklist, found here, acts as a more generalized approach to planning a campaign and information needed.

In the upcoming tasks, we will go further in-depth with these plans, documentation, and specifics of each as we take a deep dive into campaign planning.

****

Answer the questions below:

Read the above and move on to engagement documentation.

No Answer Needed

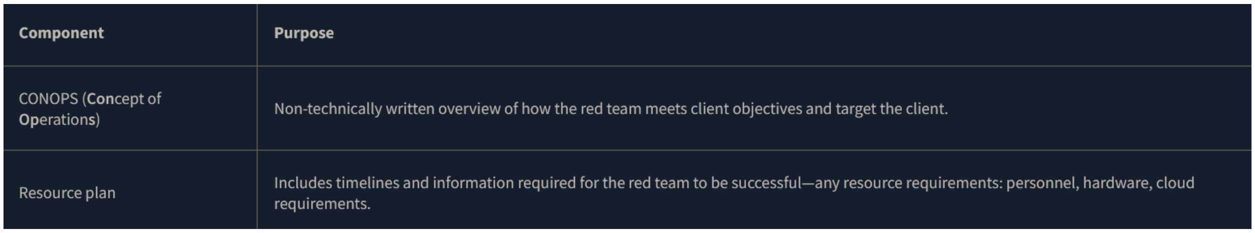
****

Engagement Documentation

Engagement documentation is an extension of campaign planning where ideas and thoughts of campaign planning are officially documented. In this context, the term "document" can be deceiving as some plans do not require proper documentation and can be as simple as an email; this will be covered later in this task.

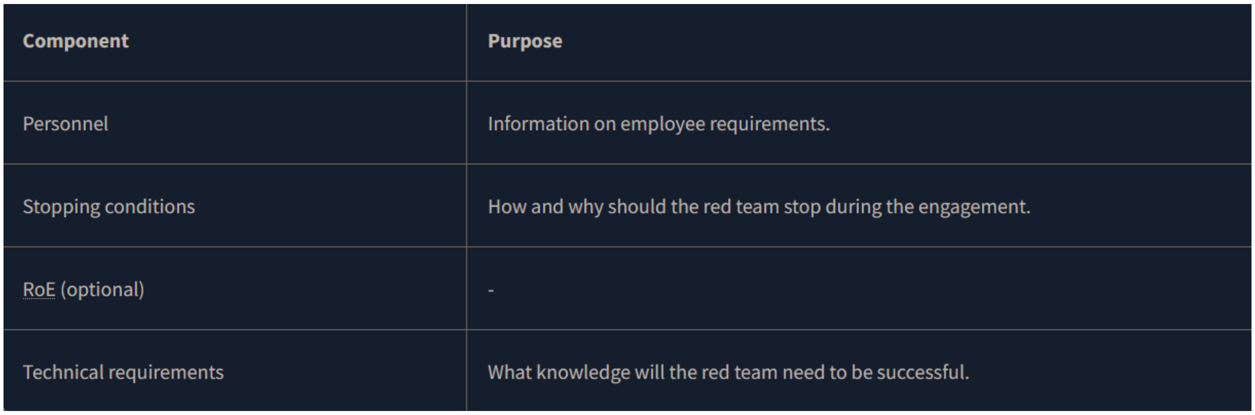
In this task, we will cover a technical overview of the contents of each campaign plan prior to looking at the plans and documents themselves in upcoming tasks.

Engagement Plan:



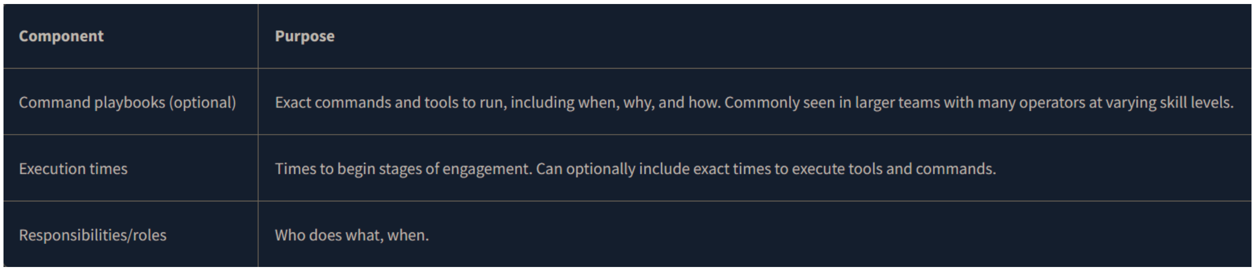
Component	Purpose
CONOPS (**Con**cept of **Op**erations)	Non-technically written overview of how the red team meets client objectives and target the client.
Resource plan	Includes timelines and information required for the red team to be successful—any resource requirements: personnel, hardware, cloud requirements.

Operations Plan:



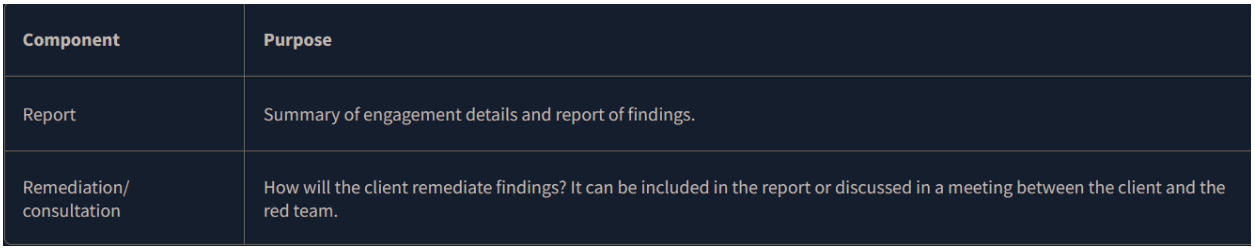
Component	Purpose
Personnel	Information on employee requirements.
Stopping conditions	How and why should the red team stop during the engagement.
RoE (optional)	-
Technical requirements	What knowledge will the red team need to be successful.

Mission Plan:



Component	Purpose
Command playbooks (optional)	Exact commands and tools to run, including when, why, and how. Commonly seen in larger teams with many operators at varying skill levels.
Execution times	Times to begin stages of engagement. Can optionally include exact times to execute tools and commands.
Responsibilities/roles	Who does what, when.

Remediation Plan (optional):



Component	Purpose
Report	Summary of engagement details and report of findings.
Remediation/ consultation	How will the client remediate findings? It can be included in the report or discussed in a meeting between the client and the red team.

****

Answer the questions below:

Read the above and move on to the upcoming engagement specific tasks.
No Answer Needed
****

Concepts of Operations

The Concept of Operation (CONOPS) is a part of the engagement plan that details a high-level overview of the proceedings of an engagement; we can compare this to an executive summary of a penetration test report. The document will serve as a business/client reference and a reference for the red cell to build off of and extend to further campaign plans.

The CONOPS document should be written from a semi-technical summary perspective, assuming the target audience/reader has zero to minimal technical knowledge. Although the CONOPS should be written at a high level, you should not omit details such as common tooling, target group, etc. As with most red team documents, there is not a set standard of a CONOPS document; below is an outline of critical components that should be included in a CONOPS

- Client Name
- Service Provider
- Timeframe
- General Objectives/Phases
- Other Training Objectives (Exfiltration)
- High-Level Tools/Techniques planned to be used
- Threat group to emulate (if any)

The key to writing and understanding a CONOPS is to provide just enough information to get a general understanding of all on-goings. The CONOPS should be easy to read and show clear definitions and points that readers can easily digest.
****

Answer the questions below:

Read the example CONOPS and answer the questions below.
No Answer Needed

Below is an example of the CONOPS for a mature organization with a strong security posture.

Example 1 - Holo Enterprises:

CONOPS:
Holo Enterprises has hired TryHackMe as an external contractor to conduct a month-long network infrastructure assessment and security posture. The campaign will utilize an assumed breach model starting in Tier 3 infrastructure. Operators will progressively conduct reconnaissance and attempt to meet objectives to be determined. If defined goals are not met, the red cell will move and escalate privileges within the network laterally. Operators are also expected to execute and maintain persistence to sustain for a period of three weeks. A trusted agent is expected to intervene if the red cell is identified or burned by the blue cell throughout the entirety of the engagement. The last engagement day is reserved for clean-up and remediation and consultation with the blue and white cell.

The customer has requested the following training objectives: assess the blue team's ability to identify and defend against live intrusions and attacks, identify the risk of an adversary within the internal network. The red cell will accomplish objectives by employing the use of Cobalt Strike as the primary red cell tool. The red cell is permitted to use other standard tooling only identifiable to the targeted threat.

Based on customer security posture and maturity, the TTP of the threat group: FIN6, will be employed throughout the engagement.

How long will the engagement last?
Answer: 1 month

How long is the red cell expected to maintain persistence?
Answer: 3 weeks

What is the primary tool used within the engagement?

Answer: Cobalt Strike
****

Resource Plan

The resource plan is the second document of the engagement plan, detailing a brief overview of dates, knowledge required (optional), resource requirements. The plan extends the CONOPS and includes specific details, such as dates, knowledge required, etc.

Unlike the CONOPS, the resource plan should not be written as a summary; instead, written as bulleted lists of subsections. As with most red team documents, there is no standard set of resource plan templates or documents; below is an outline of example subsections of the resource plan.

- Header
    - Personnel writing
    - Dates
    - Customer

- Engagement Dates
    - Reconnaissance Dates
    - Initial Compromise Dates
    - Post-Exploitation and Persistence Dates
    - Misc. Dates

- Knowledge Required(optional)
    - Reconnaissance
    - Initial Compromise
    - Post-Exploitation

- Resource Requirements
    - Personnel
    - Hardware
    - Cloud
    - Misc.

The key to writing and understanding a resource plan is to provide enough information to gather what is required but not become overbearing. The document should be straight to the point and define what is needed.

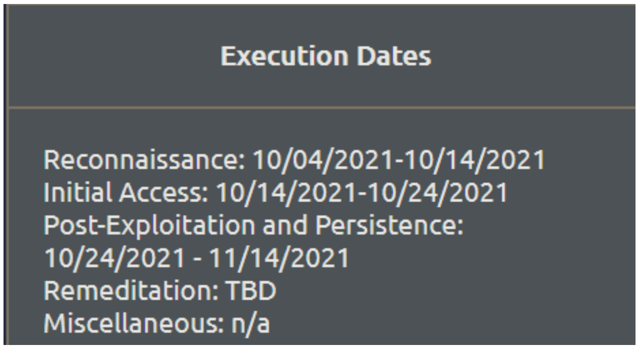
****

Answer the questions below:

Navigate to the "View Site" button and read the provided resource plan. Once complete, answer the questions below.

No Answer Needed

When will the engagement end? (MM/DD/YYYY)

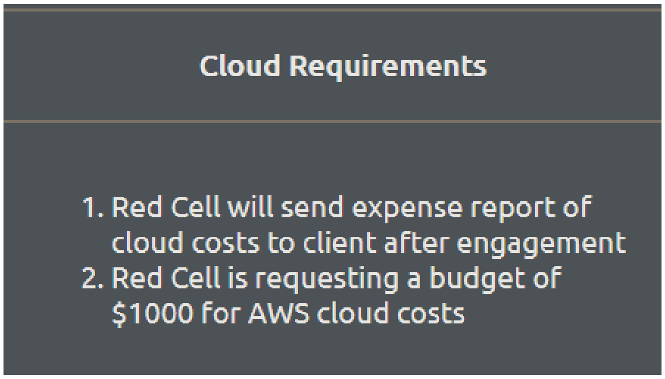


Execution Dates

Reconnaissance: 10/04/2021-10/14/2021
Initial Access: 10/14/2021-10/24/2021
Post-Exploitation and Persistence:
10/24/2021 - 11/14/2021
Remeditation: TBD
Miscellaneous: n/a

Answer: 11/14/2021

What is the budget the red team has for AWS cloud cost?

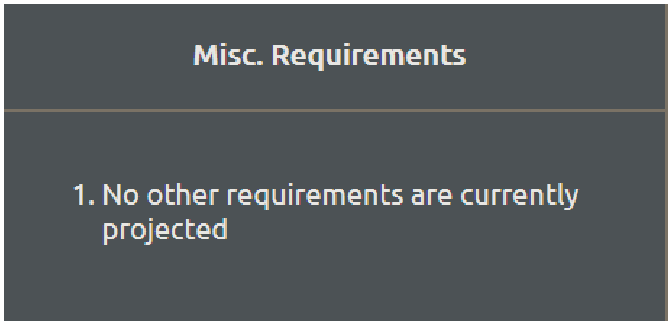


Cloud Requirements

1. Red Cell will send expense report of cloud costs to client after engagement
2. Red Cell is requesting a budget of $1000 for AWS cloud costs

Answer: $1000

Are there any miscellaneous requirements for the engagement? (Y/N)



Misc. Requirements

1. No other requirements are currently projected

Answer: N
****

Operations Plan

The operations plan is a flexible document(s) that provides specific details of the engagement and actions occurring. The plan expands upon the current CONOPS and should include a majority of specific engagement information; the ROE can also be placed here depending on the depth and structure of the ROE.

The operations plan should follow a similar writing scheme to the resource plan, using bulleted lists and small sub-sections. As with the other red team documents, there is no standard set of operation plan templates or documents; below is an outline of example subsections within the operations plan.

- Header
    - Personnel writing
    - Dates
    - Customer
- Halting/stopping conditions (can be placed in ROE depending on depth)
- Required/assigned personnel
- Specific TTPs and attacks planned
- Communications plan
- Rules of Engagement (optional)

The most notable addition to this document is the communications plan. The communications plan should summarize how the red cell will communicate with other cells and the client overall. Each team will have its preferred method to communicate with clients. Below is a list of possible options a team will choose to communicate.

- vectr.io
- Email
- Slack

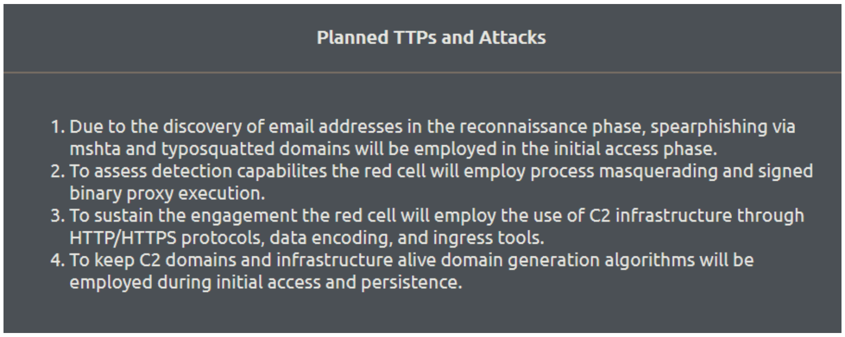
****

Answer the questions below:

Navigate to the "View Site" button and read the provided operations plan. Once complete, answer the questions below.

No Answer Needed

What phishing method will be employed during the initial access phase?

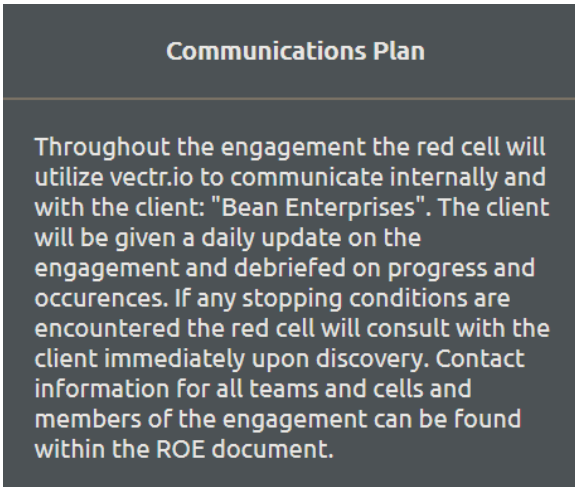


Planned TTPs and Attacks

1. Due to the discovery of email addresses in the reconnaissance phase, spearphishing via mshta and typosquatted domains will be employed in the initial access phase.
2. To assess detection capabilites the red cell will employ process masquerading and signed binary proxy execution.
3. To sustain the engagement the red cell will employ the use of C2 infrastructure through HTTP/HTTPS protocols, data encoding, and ingress tools.
4. To keep C2 domains and infrastructure alive domain generation algorithms will be employed during initial access and persistence.

Answer: Spearphishing

What site will be utilized for communication between the client and red cell?

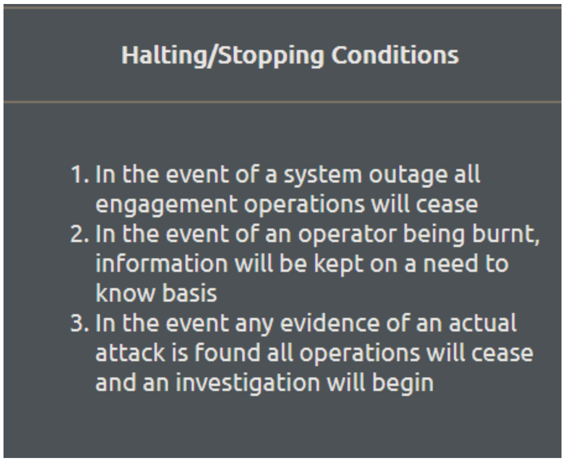


Communications Plan

Throughout the engagement the red cell will utilize vectr.io to communicate internally and with the client: "Bean Enterprises". The client will be given a daily update on the engagement and debriefed on progress and occurences. If any stopping conditions are encountered the red cell will consult with the client immediately upon discovery. Contact information for all teams and cells and members of the engagement can be found within the ROE document.

Answer: vectr.io

If there is a system outage, the red cell will continue with the engagement. (T/F)



Halting/Stopping Conditions

1. In the event of a system outage all engagement operations will cease
2. In the event of an operator being burnt, information will be kept on a need to know basis
3. In the event any evidence of an actual attack is found all operations will cease and an investigation will begin

Answer: F
****

Mission Plan

The mission plan is a cell-specific document that details the exact actions to be completed by operators. The document uses information from previous plans and assigns actions to them.

How the document is written and detailed will depend on the team; as this is an internally used document, the structure and detail have less impact. As with all the documents outlined in this room, presentation can vary; this plan can be as simple as emailing all operators. Below is a list of the minimum details that cells should include within the plan.

- Objectives
- Operators
- Exploits/Attacks
- Targets (users/machines/objectives)
- Execution plan variations

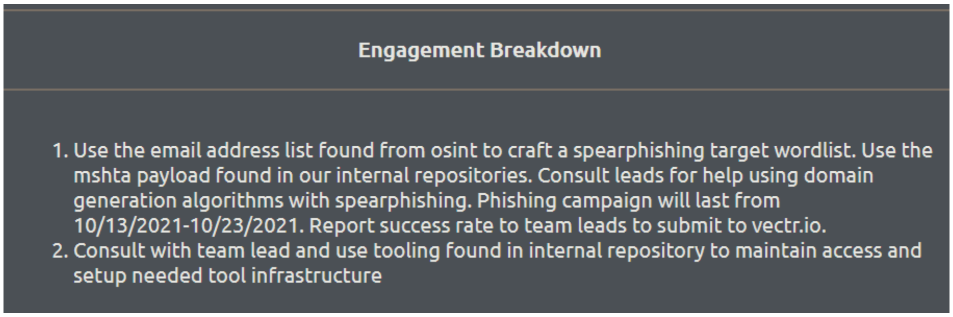
The two plans can be thought of similarly; the operations plan should be considered from a business and client perspective, and the mission plan should be thought of from an operator and red cell perspective.
****

Answer the questions below:

Navigate to the "View Site" button and read the provided mission plan. Once complete, answer the questions below.

No Answer Needed

When will the phishing campaign end? (mm/dd/yyyy)

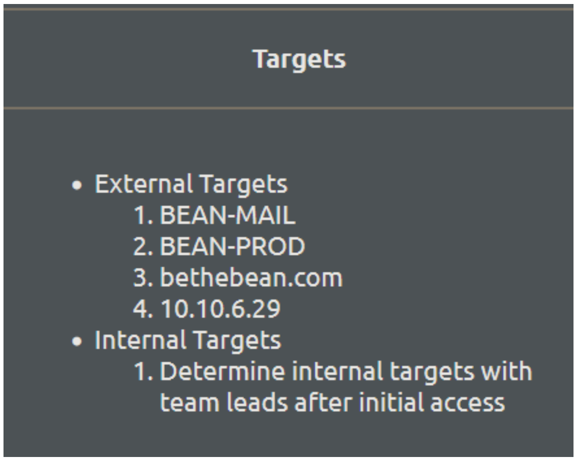


Engagement Breakdown

1. Use the email address list found from osint to craft a spearphishing target wordlist. Use the mshta payload found in our internal repositories. Consult leads for help using domain generation algorithms with spearphishing. Phishing campaign will last from 10/13/2021-10/23/2021. Report success rate to team leads to submit to vectr.io.
2. Consult with team lead and use tooling found in internal repository to maintain access and setup needed tool infrastructure

Answer: 10/23/2021

Are you permitted to attack 10.10.6.78? (Y/N)

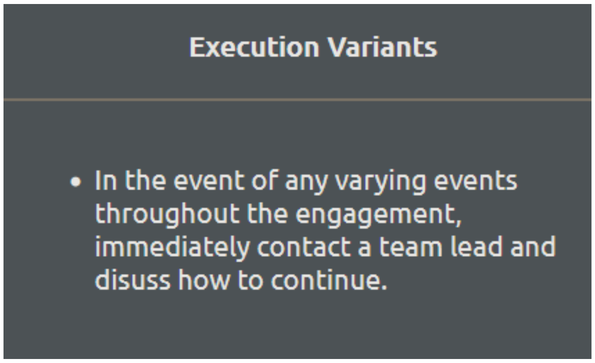


Targets

- External Targets
  1. BEAN-MAIL
  2. BEAN-PROD
  3. bethebean.com
  4. 10.10.6.29
- Internal Targets
  1. Determine internal targets with team leads after initial access

Answer: N

When a stopping condition is encountered, you should continue working and determine the solution yourself without a team lead. (T/F)



Execution Variants

- In the event of any varying events throughout the engagement, immediately contact a team lead and disuss how to continue.

Answer: F

****

Conclusion

We have covered how you can quantify campaign plans into documents and prepare for a successful red team engagement in this room. The consistent theme throughout this room has been that each red team will have its internal documents and way of doing things. This is a crucial concept to understand when moving into the real world. This room only acts as a guide to get you used to concepts and ideas and provides a framework to use, not as a definitive step-by-step manual. When planning an engagement, remember that your number 1 goal is to meet the client's objectives.

Planning and documenting are often overlooked and are crucial to a successful engagement.