

# Red Team Engagements

Learn the steps and procedures of a red team engagement, including planning, frameworks, and documentation.

## Task 2 Defining Scope and Objectives

Question	Answer
What CIDR range is permitted to be attacked?	10.0.4.0/22
Is the use of white cards permitted? (Y/N)	Y
Are you permitted to access "*.bethechange.xyz?" (Y/N)	N

## Task 3 Rules of Engagement

Question	Answer
How many explicit restrictions are specified?	3
What is the first access type mentioned in the document?	Phishing
Is the red team permitted to attack 192.168.1.0/24? (Y/N)	N

## Task 6 Concept of Operations

Question	Answer
How long will the engagement last?	1 month
How long is the red cell expected to maintain persistence?	3 weeks
What is the primary tool used within the engagement?	Cobalt Strike

## Task 7 Resource Plan

→ I clicked on "view site"

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

Answer: **11/14/2021**

Resource Plan	
RED CELL LEAD: Cryillic ENGAGEMENT DATES: 10/12/21 - 11/12/21	ASST CELL LEAD: Simpuki CLIENT POC: Bean Enterprises
Execution Dates	Resource Summary
Reconnaissance: 10/04/2021-10/14/2021 Initial Access: 10/14/2021-10/24/2021 Post-Exploitation and Persistence: 10/24/2021 - <b>11/14/2021</b> Remediation: TBD Miscellaneous: n/a	The red cell has requested the needed resources outlined in the following document. Any further resources needed by any teams or operators should create a revised resource plan and submit to the client representatives for approval.
Personnel Requirements	Hardware Requirements
1. One Red Cell Lead(s) 2. One Red Cell Assistant Lead(s) 3. Three Red Cell Operators	1. No hardware is required for this engagement, all machine resources will be allocated to the cloud
Cloud Requirements	Misc Requirements

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

Answer: **\$1000**

Personnel Requirements	Hardware Requirements
<ol style="list-style-type: none"> <li>1. One Red Cell Lead(s)</li> <li>2. One Red Cell Assistant Lead(s)</li> <li>3. Three Red Cell Operators</li> </ol>	<ol style="list-style-type: none"> <li>1. No hardware is required for this engagement, all machine resources will be allocated to the cloud</li> </ol>
Cloud Requirements	Misc. Requirements
<ol style="list-style-type: none"> <li>1. Red Cell will send expense report of cloud costs to client after engagement</li> <li>2. Red Cell is requesting a budget of \$1000 for AWS cloud costs</li> </ol>	<ol style="list-style-type: none"> <li>1. No other requirements are currently projected</li> </ol>

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

Answer: N

Personnel Requirements	Hardware Requirements
<ol style="list-style-type: none"> <li>1. One Red Cell Lead(s)</li> <li>2. One Red Cell Assistant Lead(s)</li> <li>3. Three Red Cell Operators</li> </ol>	<ol style="list-style-type: none"> <li>1. No hardware is required for this engagement, all machine resources will be allocated to the cloud</li> </ol>
Cloud Requirements	Misc. Requirements
<ol style="list-style-type: none"> <li>1. Red Cell will send expense report of cloud costs to client after engagement</li> <li>2. Red Cell is requesting a budget of \$1000 for AWS cloud costs</li> </ol>	<ol style="list-style-type: none"> <li>1. No other requirements are currently projected</li> </ol>

## Task 8 Operations Plan

→ I clicked on "view site" button

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

Answer: **spear phishing**

### 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 capabilities 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.

—

Resource Plan

Operations Plan

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

Answer: **vectr.io**

Halting/Stopping Conditions	Communications Plan
<ol style="list-style-type: none"><li>1. In the event of a system outage all engagement operations will cease</li><li>2. In the event of an operator being burnt, information will be kept on a need to know basis</li><li>3. In the event any evidence of an actual attack is found all operations will cease and an investigation will begin</li></ol>	<p>Throughout the engagement the red cell will utilize <b>vectr.io</b> 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 occurrences. 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.</p>

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

Answer: **F**

Halting/Stopping Conditions	Communications Plan
<ol style="list-style-type: none"><li>1. In the event of a system outage all engagement operations will cease</li><li>2. In the event of an operator being burnt, information will be kept on a need to know basis</li><li>3. In the event any evidence of an actual attack is found all operations will cease and an investigation will begin</li></ol>	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 occurrences. 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.

## Task 9 Mission Plan


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

Answer: **10/23/2021**

Engagement Breakdown
<ol style="list-style-type: none"><li>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.</li><li>2. Consult with team lead and use tooling found in internal repository to maintain access and setup needed tool infrastructure</li></ol>



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

Answer: **N**

Targets	
<ul style="list-style-type: none"><li>• External Targets<ol style="list-style-type: none"><li>1. BEAN-MAIL</li><li>2. BEAN-PROD</li><li>3. bethebean.com</li><li>4. 10.10.6.29</li></ol></li><li>• Internal Targets<ol style="list-style-type: none"><li>1. Determine internal targets with team leads after initial access</li></ol></li></ul>	<div>NOT IN SCOPE</div> 

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

Answer: **F**

Execution Variants
<ul style="list-style-type: none"><li>• In the event of any varying events throughout the engagement, immediately contact a team lead and discuss how to continue.</li></ul>  

**END!!!**