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)	Υ
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 - 11/14/2021 Remeditation: 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	No hardware is required for this engagement, all machine resources will be allocated to the cloud	
dlpt.	4	

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

Answer: \$1000

Personnel Requirements	Hardware Requirements
1. One Red Cell Lead(s) 2. One Red Cell Assistant Lead(s) 3. Three Red Cell Operators	No hardware is required for this engagement, all machine resources will be allocated to the cloud
Cloud Requirements	Misc. 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	1. No other requirements are currently projected

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

Answer: N

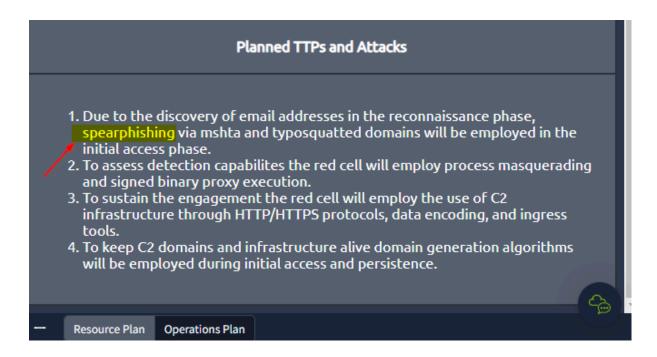
Personnel Requirements	Hardware Requirements
1. One Red Cell Lead(s) 2. One Red Cell Assistant Lead(s) 3. Three Red Cell Operators	No hardware is required for this engagement, all machine resources will be allocated to the cloud
Cloud Requirements	Misc. Requirements
 Red Cell will send expense report of cloud costs to client after engagement Red Cell is requesting a budget of \$1000 for AWS cloud costs 	1. No other requirements are currently projected

Task 8 Operations Plan

→ I clicked on "view site" button

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

Answer: spear phishing



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

Answer: vectr.io

Halting/Stopping Conditions	Communications Plan
 In the event of a system outage all engagement operations will cease In the event of an operator being burnt, information will be kept on a need to know basis In the event any evidence of an actual attack is found all operations will cease and an investigation will begin 	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.

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

Answer: F

Halting/Stopping Conditions Communications Plan Throughout the engagement the red 1. In the event of a system outage cell will utilize vectr.io to communicate all engagement operations will internally and with the client: "Bean Enterprises". The client will be given a 2. In the event of an operator being daily update on the engagement and burnt, information will be kept debriefed on progress and occurences. on a need to know basis If any stopping conditions are 3. In the event any evidence of an encountered the red cell will consult actual attack is found all with the client immediately upon operations will cease and an discovery. Contact information for all investigation will begin 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)

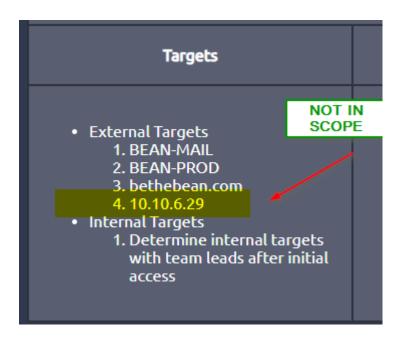
Answer: 10/23/2021

Engagement Breakdown

- 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

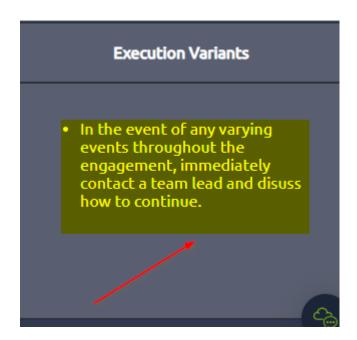
Are you permitted to attack 10.10.6.78? (Y/N)

Answer: N



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

Answer: F



END!!!