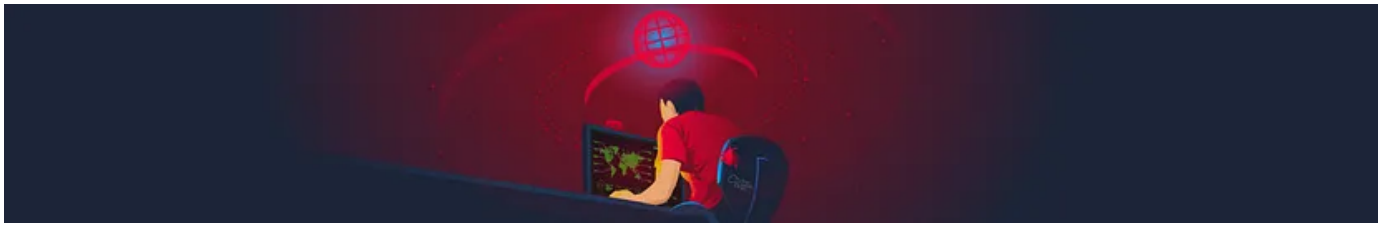
# Red Team Engagements | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Md Amiruddin · Follow
Published in InfoSec Write-ups
12 min read · Mar 18, 2023



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



## Task 1 : 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 of needs and resources available and TTPs.
- Understand how to write engagement documentation in accordance to client objectives.

This room requires no prerequisite information or knowledge.

### Task 2 : 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 :**

```
1. Read the example client objectives and answer the questions below.
A. No answer needed

2. Below is an example of the client objectives of a mature organization with a strong security posture.

Example 1 - Global Enterprises:

Objectives:

Identify system misconfigurations and network weaknesses.
Focus on exterior 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.
Use of white cards is permitted depending on downtime and length.
Evaluate the impact of data exposure and exfiltration.
Scope:

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.
Exfiltration of PII is prohibited. Use arbitrary exfiltration data.
Attacks against systems within 10.0.4.0/22 are permitted.
Attacks against systems within 10.0.12.0/22 are prohibited.
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.

A. No answer needed

3. What CIDR range is permitted to be attacked?
A. 10.0.4.0/22

4. Is the use of white cards permitted? (Y/N)
A. Y

5. Are you permitted to access "*.bethechange.xyz?" (Y/N)
A. N
```

## Task 3 : 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 (**N**on-**D**isclosure **A**greement) 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.

Downloaded Task files are shown below -

TryHackMe


# Rules of Engagement

Global Enterprises
1/17/2022

## Executive Summary

The Rules of Engagement (ROE) document the approvals, authorizations, and critical implementation issues necessary to execute the engagement. Signing of the ROE constitutes acknowledgement and approval of the customer, system owner, and Red Team of the Red Team's authorities in execution of the engagement.

The objectives include:

- Monitor security posture and response
  - Focus on internal systems and insider threats
- Assess the response of the defense team
- Assess ability to move laterally through internal infrastructure
- Employ physical penetration testing to assess onsite security posture

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

Authorized Target Space:

- 10.0.4.0/22
- *.bethechange.xyz, *.globalenterprises.thm

Activities:

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

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.

1. Once downloaded, read the sample document and answer the questions below.
A. No answer needed

2. How many explicit restriction are specified?
A. 3

3. What is the first access type mentioned in the document?
A. Phishing

4. Is the red team permitted to attack 192.168.1.0/24? (Y/N)
A. N
```

## Task 4 : 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 :**

```
1. Read the above and move on to engagement documentation.
A. No answer needed
```

## Task 5 : 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 (Concept of Operations) | 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. |

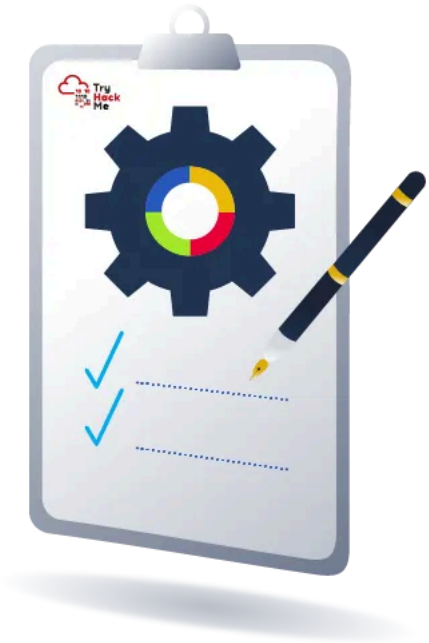
**Remediation Plan (optional):**

| 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 :**

```
1. Read the above and move on to upcoming engagement specific tasks.
A. No answer needed
```

### Task 6 : Concept 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 :**

```
1. Read the example CONOPS and answer the questions below.
A. No answer needed

2. 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 an
The customer has requested the following training objectives: assess the blue team's ability to identify and defend against
Based on customer security posture and maturity, the TTP of the threat group: FIN6, will be employed throughout the engagem

A. No answer needed

3. How long will the engagement last?
A. 1 Month

4. How long is the red cell expected to maintain persistence?
A. 3 Weeks

5. What is the primary tool used within the engagement?
A. Cobalt Strike
```

## Task 7 : 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

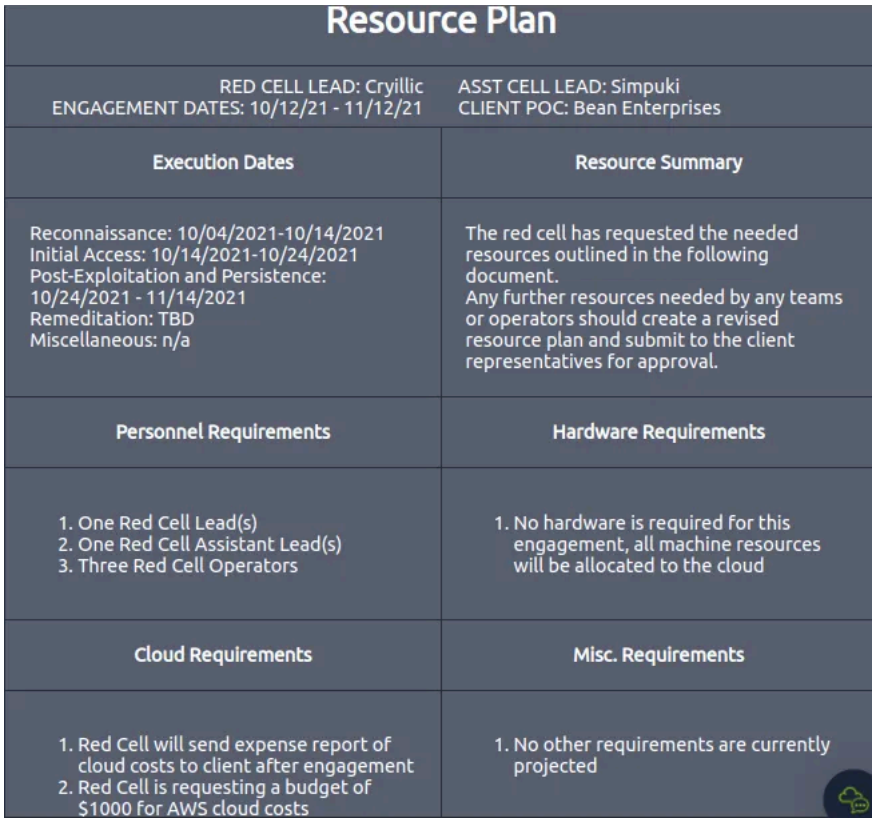
**Knowledge Required (optional)**

- 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.



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<br>Initial Access: 10/14/2021-10/24/2021<br>Post-Exploitation and Persistence: 10/24/2021 - 11/14/2021<br>Remeditation: TBD<br>Miscellaneous: n/a | The red cell has requested the needed resources outlined in the following document.<br>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)<br>2. One Red Cell Assistant Lead(s)<br>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** |
| 1. Red Cell will send expense report of cloud costs to client after engagement<br>2. Red Cell is requesting a budget of $1000 for AWS cloud costs | 1. No other requirements are currently projected |

**Answer the questions below :**

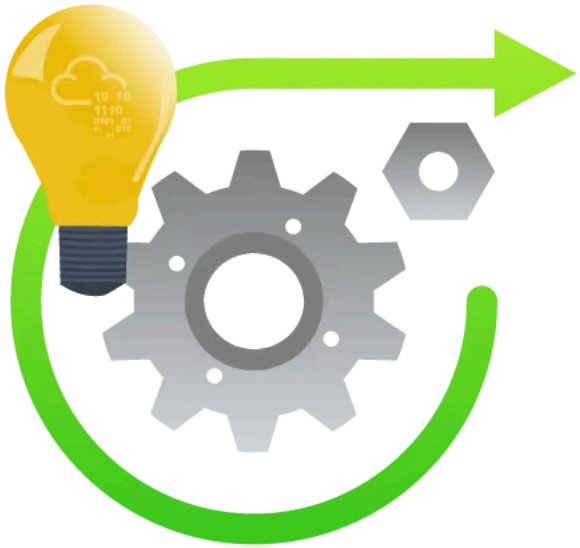
```
1. Navigate to the "View Site"  button and read the provided resource plan. Once complete, answer the questions below.
A. No answer needed

2. When will the engagement end? (MM/DD/YYYY)
A. 11/14/2021

3. What is the budget the red team has for AWS cloud cost?
A. $1000

4. Are there any miscellaneous requirements for the engagement? (Y/N)
A. N
```

## Task 8 : 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**

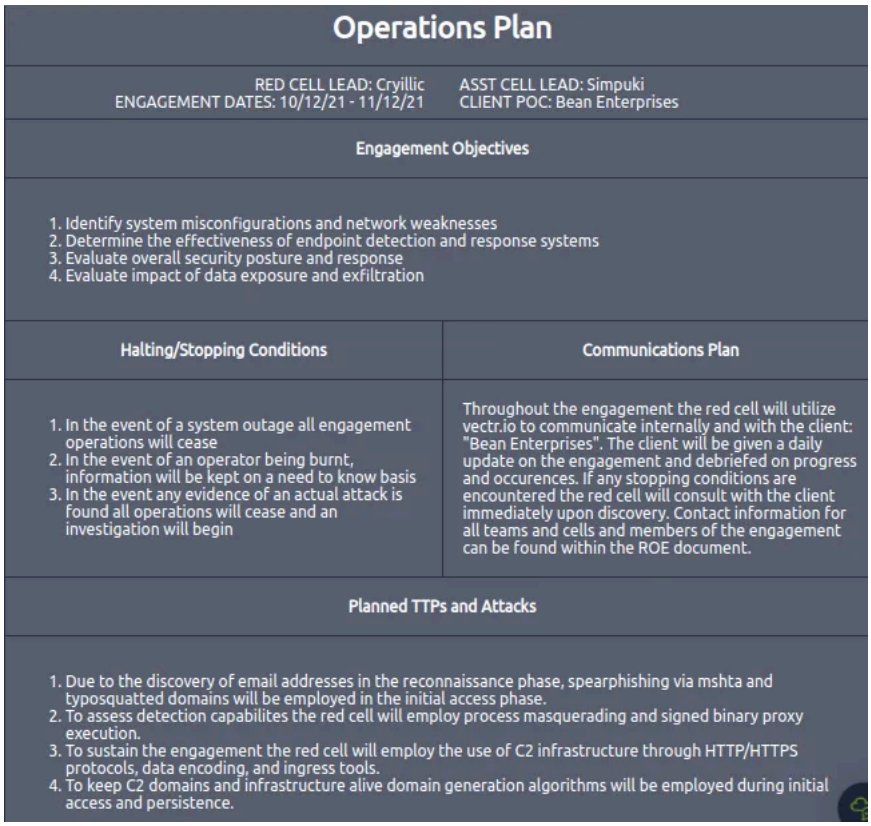
- Personnel writing
- Dates
- Customer

**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 :**

```
1. Navigate to the "View Site"  button and read the provided operations plan. Once complete, answer the questions below.
A. No answer needed

2. What phishing method will be employed during the initial access phase?
A. Spearphishing

3. What site will be utilized for communication between the client and red cell?
A. vectr.io

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

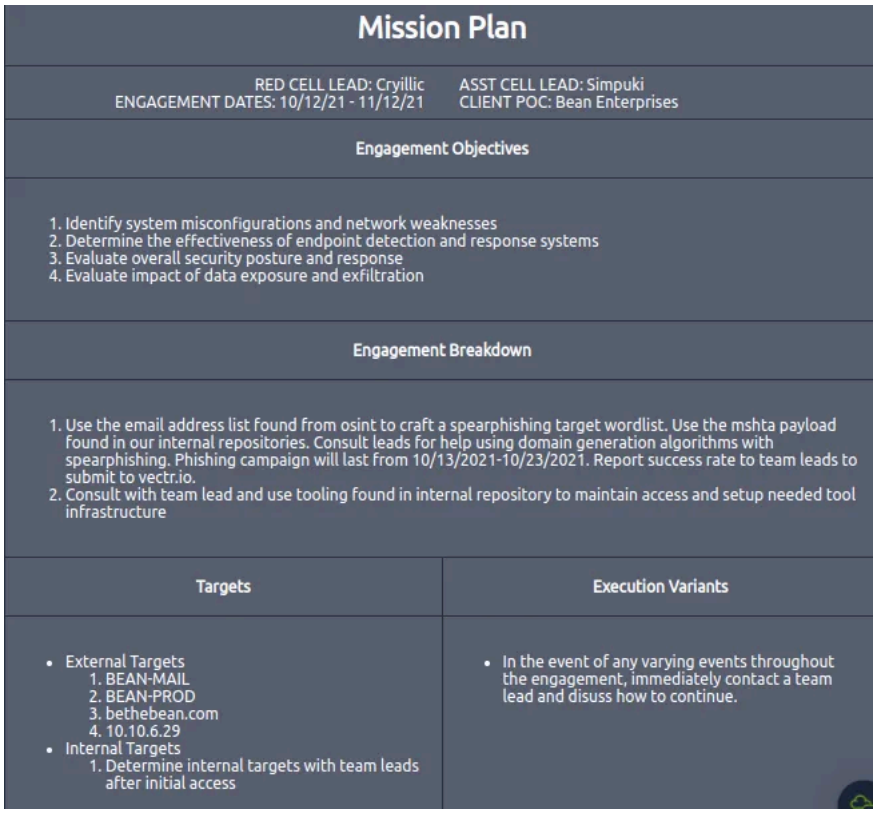
## Task 9 : Mission Plan

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 detail 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 :**

```
1. Navigate to the "View Site"  button and read the provided mission plan. Once complete, answer the questions below.
A. No answer needed

2. When will the phishing campaign end? (mm/dd/yyyy)
A. 10/23/2021

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

4. When a stopping condition is encountered, you should continue working and determine the solution yourself without a team
A. F
```

## Task 10 : 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.

**Thankyou For Reading.**

Tryhackme | Tryhackme Walkthrough | Cybersecurity | Infosec | Information Security

Follow

## Published in InfoSec Write-ups

49K Followers · Last published 1 day ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Follow

## Written by Md Amiruddin

155 Followers · 6 Following

This is a profile of a cybersecurity enthusiast and CTF writer. He is an experienced information security professional and highly motivated individual.

### No responses yet

What are your thoughts?

Respond

### More from the list: "Tryhackme Writeup/Walkthrough"

Curated by Md Amiruddin

In InfoSec W... by Md Ami...
**SDLC (Software Development Lifecycle) ...**
Apr 10, 2023

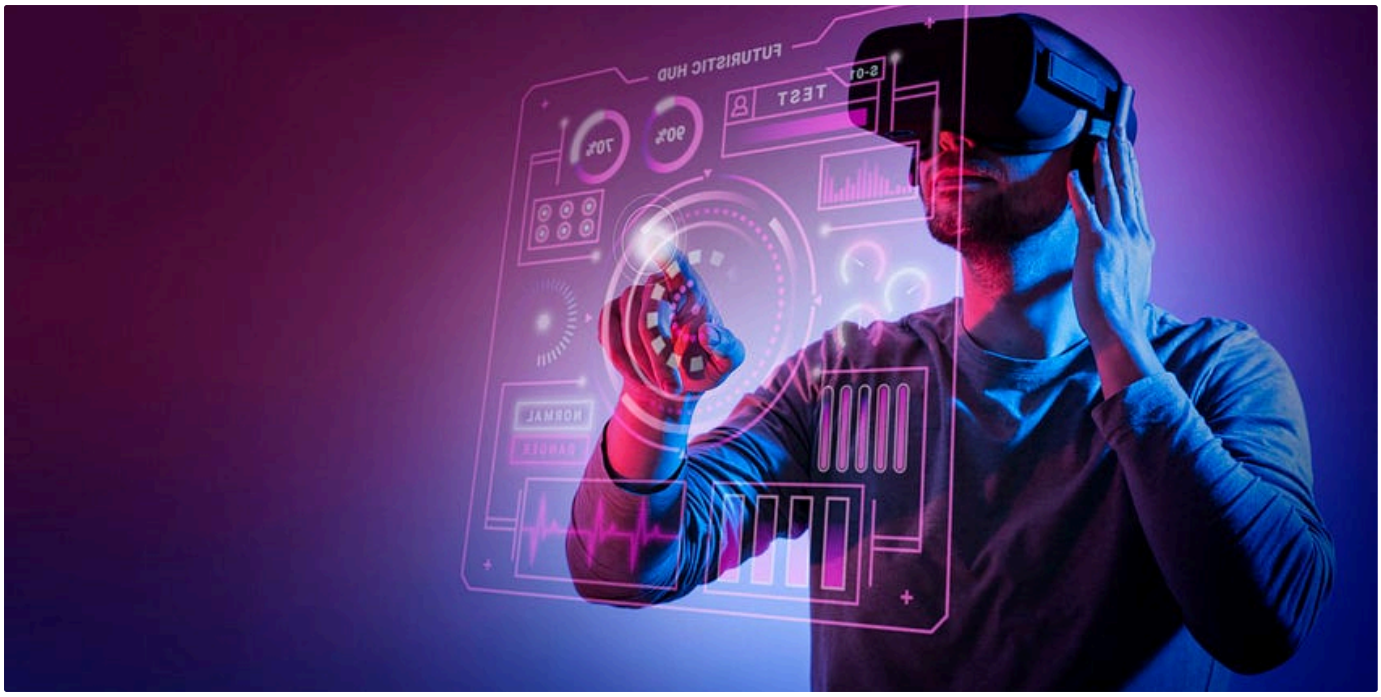
In InfoSec W... by Md Ami...
**Outlook NTLM Leak | Tryhackme...**
Mar 24, 2023

In InfoSec W... by Md Ami...
**MITRE | Tryhackme Room Writeup/Walkthrough |...**
Mar 20, 2023

In InfoSec W... by Md Ami...
**Red Team Fundamentals Tryhackme...**
Mar 16, 2023

View list

### More from Md Amiruddin and InfoSec Write-ups

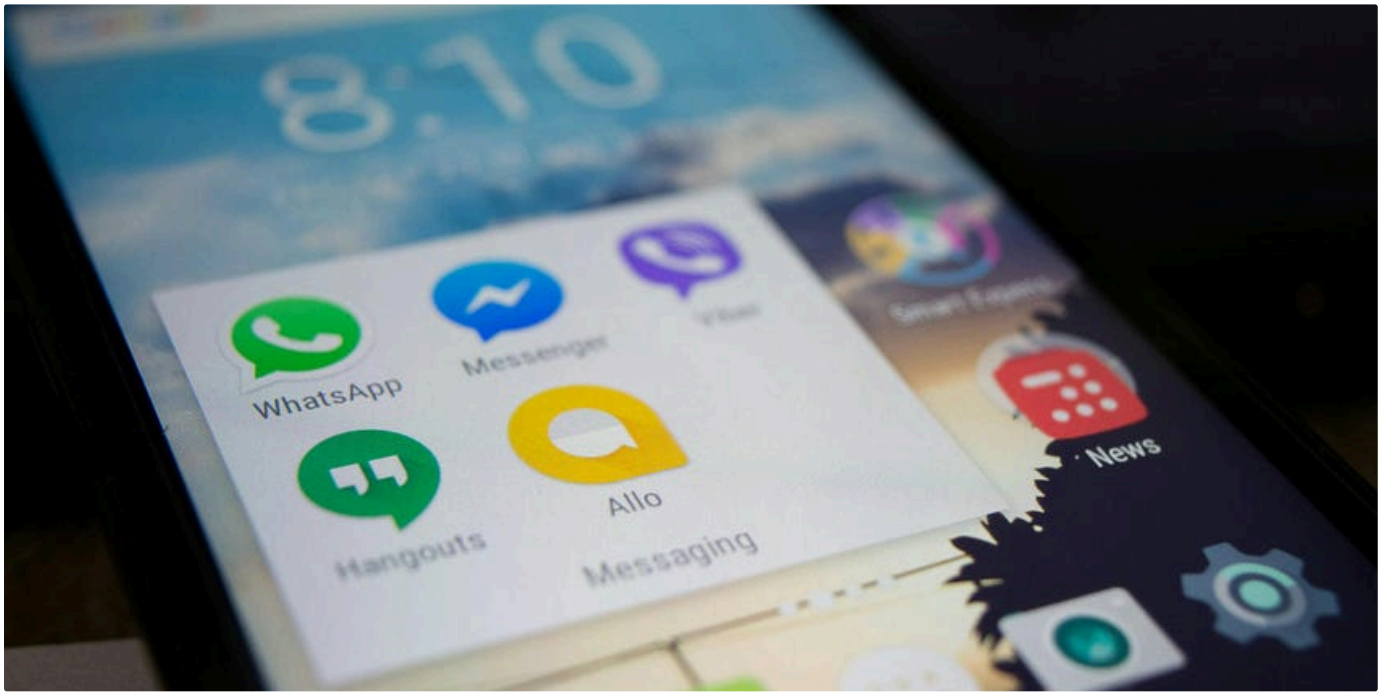



In InfoSec Write-ups by Md Amiruddin

## Vulnhub Writeup/Walkthrough SickOS 1.1 | By Md Amiruddin

This CTF walkthrough is similar to the labs found in the OSCP exam course.

Dec 21, 2022




In InfoSec Write-ups by Visir

## Could You Be the Next Victim? How to Protect Your Google Account Now

Today, nearly everyone is connected to the internet, and this dependency grew exponentially during the COVID-19 pandemic. With more people...

6d ago 15


In InfoSec Write-ups by Shanzah Shahid

## Hack Like a Pro: Mastering Penetration Testing with Virtual vs Physical Lab Setups

Learn how to build a powerful, cost-effective testing environment to sharpen your ethical hacking skills.

2d ago 44 2

In InfoSec Write-ups by Md Amiruddin

## Intro to Containerisation | Tryhackme Writeup/Walkthrough | by Md Amiruddin

This is a writeup/walkthrough of Tryhackme room “Intro to Containerisation” by Md Amiruddin

Feb 12, 2023 19

See all from Md Amiruddin

See all from InfoSec Write-ups

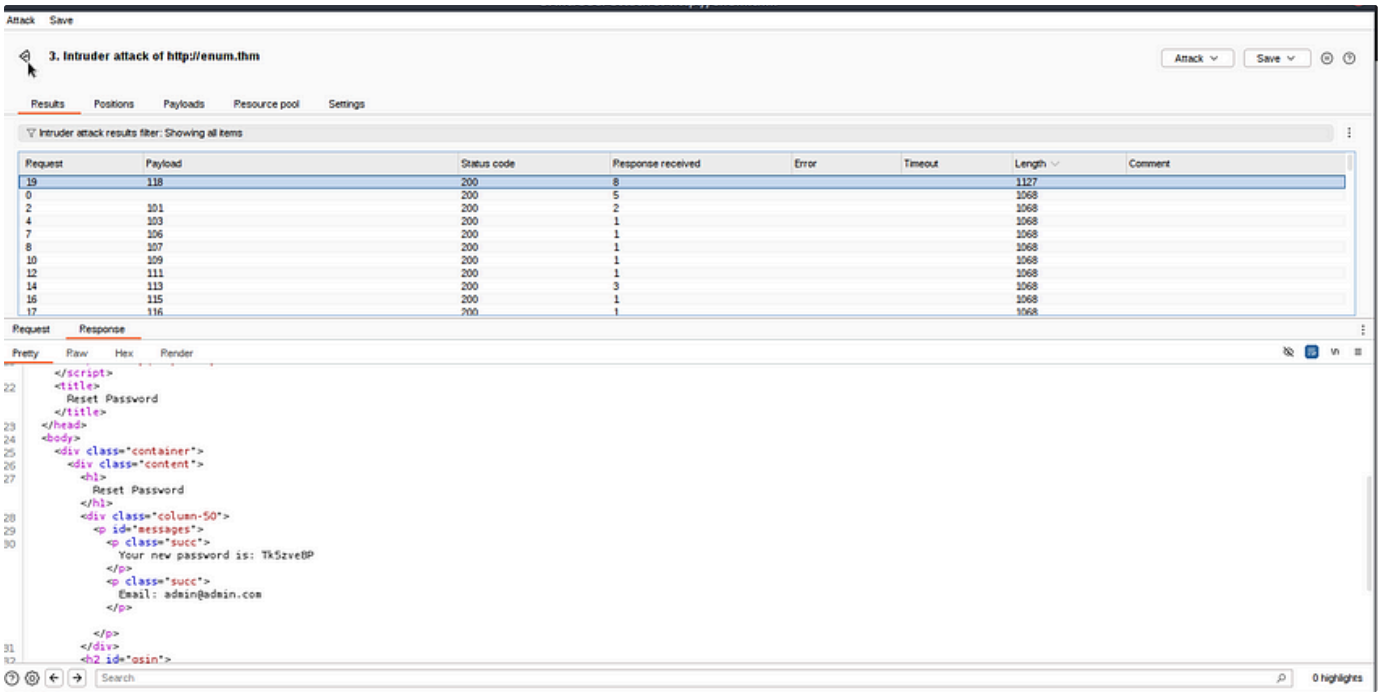
## Recommended from Medium


Sudarshan Patel

**Tryhackme | Advent of Cyber—2024 | Day 3: Even if I wanted to go, their vulnerabilities wouldn't...**

The Story

Dec 5, 2024 38



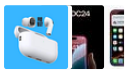

embossdotar

## TryHackMe—Enumeration & Brute Force—Writeup

Key points: Enumeration | Brute Force | Exploring Authentication Mechanisms | Common Places to Enumerate | Verbose Errors | Password Reset...

Jul 31, 2024 26

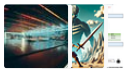
### Lists



**Tech & Tools**
22 stories · 377 saves

**Medium's Huge List of Publications Accepting Submissions**
377 stories · 4315 saves

**Staff picks**
793 stories · 1546 saves



**Natural Language Processing**
1882 stories · 1520 saves


Angie

### CI/CD and Build Security TryHackMe Writeup | THM Walkthrough

Hello everyone! In today's post, I will walk you through TryHackMe's CI/CD and Build Security room. This is part of the DevSecOps learning...

Jul 17, 2024 51 1


Abhijeet Singh

### Advent of Cyber 2024 [Day 3] Even if I wanted to go, their vulnerabilities wouldn't allow it.

So, Let's Start with the Questions. I hope you already read the story and all the given instructions —

Dec 4, 2024 2

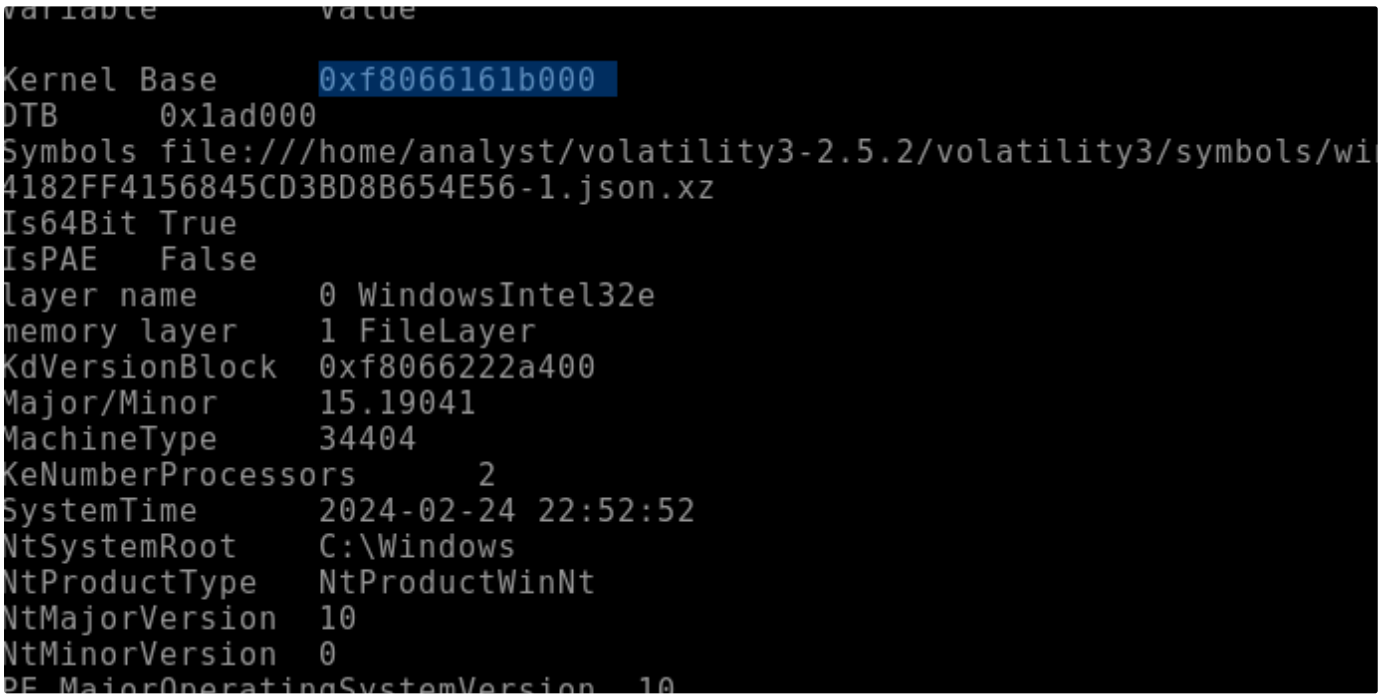


In InfoSec Write-ups by Karthikeyan Nagaraj

### Advent of Cyber 2024 [ Day 4] Writeup with Answers | TryHackMe Walkthrough

I'm all atomic inside!

Dec 4, 2024 882 1




embossdotar

### TryHackMe—Critical—Writeup

Key points: Memory dump | Memory Forensics | Computer Forensics | Random Access Memory | RAM | FTK Imager | Volatility 3 | vol | Analyst...

Jul 18, 2024 16

See more recommendations