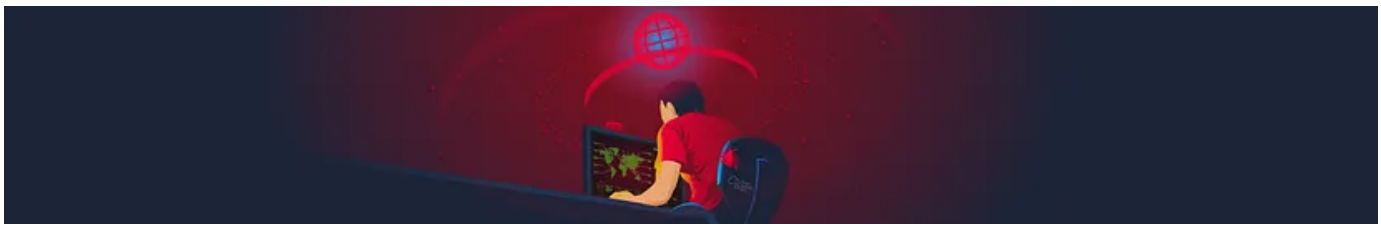
Red Team Fundamentals | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Md Amiruddin · Follow
Published in InfoSec Write-ups
12 min read · Mar 16, 2023

Learn about the basics of a red engagement, the main components and stakeholders involved, and how red teaming differs from other cyber security engagements.



Task 1 : Introduction

Cybersecurity is a constant race between white hat hackers and black hat hackers. As threats in the cyber-world evolve, so does the need for more specialized services that allow companies to prepare for real attacks the best they can.

While conventional security engagements like vulnerability assessments and penetration tests could provide an excellent overview of the technical security posture of a company, they might overlook some other aspects that a real attacker can exploit. In that sense, we could say that conventional penetration tests are good at showing vulnerabilities so that you can take proactive measures but might not teach you how to respond to an actual ongoing attack by a motivated adversary.

Room objectives

- Learn about the basics of red team engagements
- Identify the main components and stakeholders involved in a red team engagement
- Understand the main differences between red teaming and other types of cybersecurity engagements

Room prerequisites

Before beginning this room, familiarity with general hacking techniques is required. Although not strictly necessary, completing the Jr. Penetration Tester Learning Path is recommended.

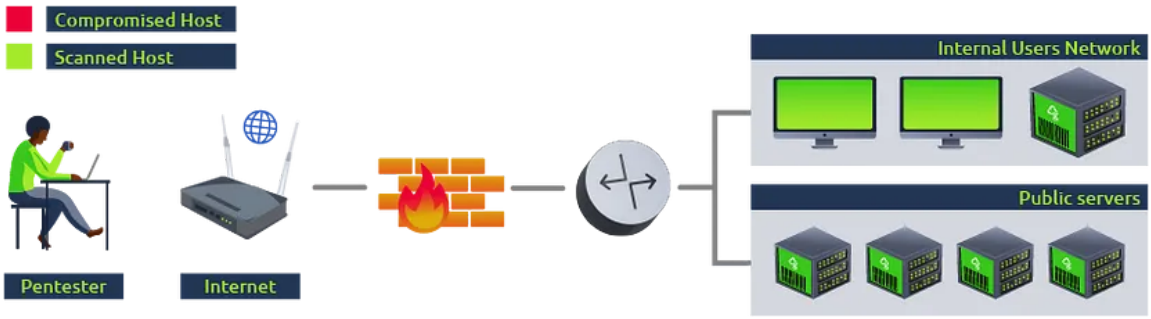
Task 2 : Vulnerability Assessment and Penetration Tests Limitations

Vulnerability Assessments

This is the simplest form of security assessment, and its main objective is to identify as many vulnerabilities in as many systems in the network as possible. To this end, concessions may be made to meet this goal effectively. For example, the attacker's machine may be allowlisted on the available security solutions to avoid interfering with the vulnerability discovery process. This makes sense since the objective is to look at every host on the network and evaluate its security posture individually while providing the most information to the company about where to focus its remediation efforts.

To summarize, a vulnerability assessment focuses on scanning hosts for vulnerabilities as individual entities so that security deficiencies can be **identified** and effective security measures can be deployed to **protect** the network in a prioritized manner. Most of the work can be done with automated tools and performed by operators without requiring much technical knowledge.

As an example, if you were to run a vulnerability assessment over a network, you would normally try to scan as many of the hosts as possible, but wouldn't actually try exploiting any vulnerabilities at all:



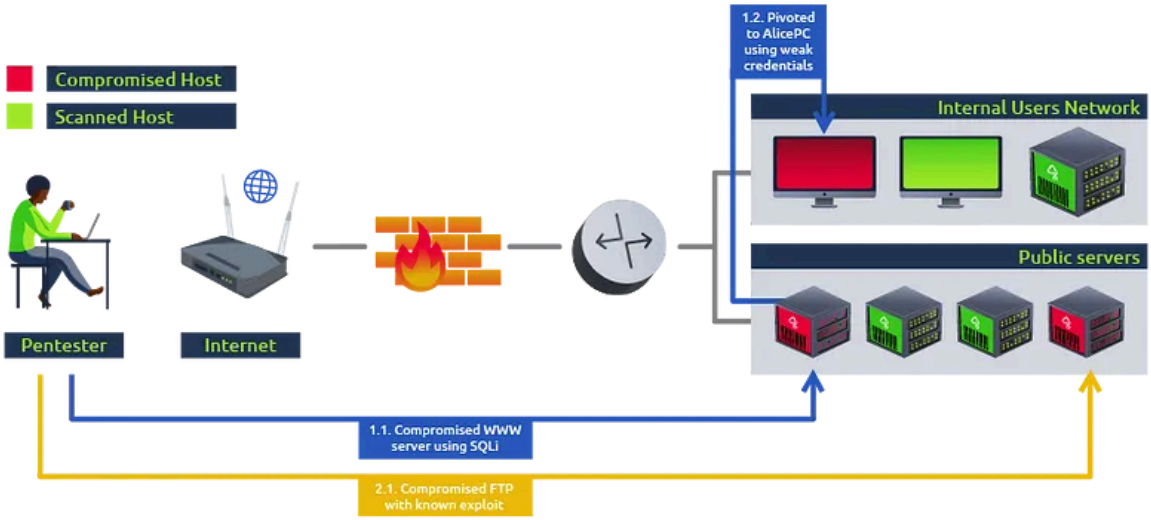
Penetration Tests

On top of scanning every single host for vulnerabilities, we often need to understand how they impact our network as a whole. Penetration tests add to vulnerability assessments by allowing the pentester to explore the impact of an attacker on the overall network by doing additional steps that include:

- Attempt to **exploit** the vulnerabilities found on each system. This is important as sometimes a vulnerability might exist in a system, but compensatory controls in place effectively prevent its exploitation. It also allows us to test if we can use the detected vulnerabilities to compromise a given host.
- Conduct **post-exploitation** tasks on any compromised host, allowing us to find if we can extract any helpful information from them or if we might use them to pivot to other hosts that were not previously accessible from where we stand.

Penetration tests might start by scanning for vulnerabilities just as a regular vulnerability assessment but provide further information on how an attacker can chain vulnerabilities to achieve specific goals. While its focus remains on **identifying** vulnerabilities and establishing measures to **protect** the network, it also considers the network as a whole ecosystem and how an attacker could profit from interactions between its components.

If we were to perform a penetration test using the same example network as before, on top of scanning all of the hosts on the network for vulnerabilities we would try confirm if they can be exploited in order to show the impact an attacker could have on the network:



By analyzing how an attacker could move around our network, we also gain a basic insight on possible security measure bypasses and our ability to **detect** a real threat actor to a certain extent, limited because the scope of a penetration test is usually extensive and Penetration testers don't care much about being loud or generating lots of alerts on security devices since time constraints on such projects often requires us to check the network in a short time.

Advanced Persistent Threats and why Regular Pentesting is not Enough

While the conventional security engagements we have mentioned cover the finding of most technical vulnerabilities, there are limitations on such processes and the extent to which they can effectively prepare a company against a real attacker. Such limitations include:

As a consequence, some aspects of penetration tests might significantly differ from a real attack, like:

- **Penetration tests are LOUD:** Usually, pentesters won't put much effort into trying to go undetected. Unlike real attackers, they don't mind being easy to detect, as they have been contracted to find as many vulnerabilities as they can in as many hosts as possible.
- **Non-technical attack vectors might be overlooked:** Attacks based on social engineering or physical intrusions are usually not included in what is tested.
- **Relaxation of security mechanisms:** While doing a regular penetration test, some security mechanisms might be temporarily disabled or relaxed for the pentesting team in favor of efficiency. Although this might sound counterintuitive, it is essential to remember that pentesters have limited time to check the network. Therefore, it is usually desired not to waste their time searching for exotic ways to bypass IDS/IPS, WAF, intrusion deception or other security measures, but rather focus on reviewing critical technological infrastructure for vulnerabilities.

On the other hand, real attackers won't follow an ethical code and are mostly unrestricted in their actions. Nowadays, the most prominent threat actors are known as **Advanced Persistent Threats (APT)**, which are highly skilled groups of attackers, usually sponsored by nations or organised criminal groups. They primarily target critical infrastructure, financial organisations, and government institutions. They are called persistent because the operations of these groups can remain undetected on compromised networks for long periods.

If a company is affected by an APT, would it be prepared to respond effectively? Could they detect the methods used to gain and maintain access on their networks if the attacker has been there for several months? What if the initial access was obtained

because John at accounting opened a suspicious email attachment? What if a zero-day exploit was involved? Do previous penetration tests prepare us for this?

To provide a more realistic approach to security, red team Engagements were born.

Answer the questions below :

```
1. Would vulnerability assessments prepare us to detect a real attacker on our networks? (Yay/Nay)
A. Nay

2. During a penetration test, are you concerned about being detected by the client? (Yay/Nay)
A. Nay

3. Highly organised groups of skilled attackers are nowadays referred to as ...
A. Advanced Persistent Threats
```

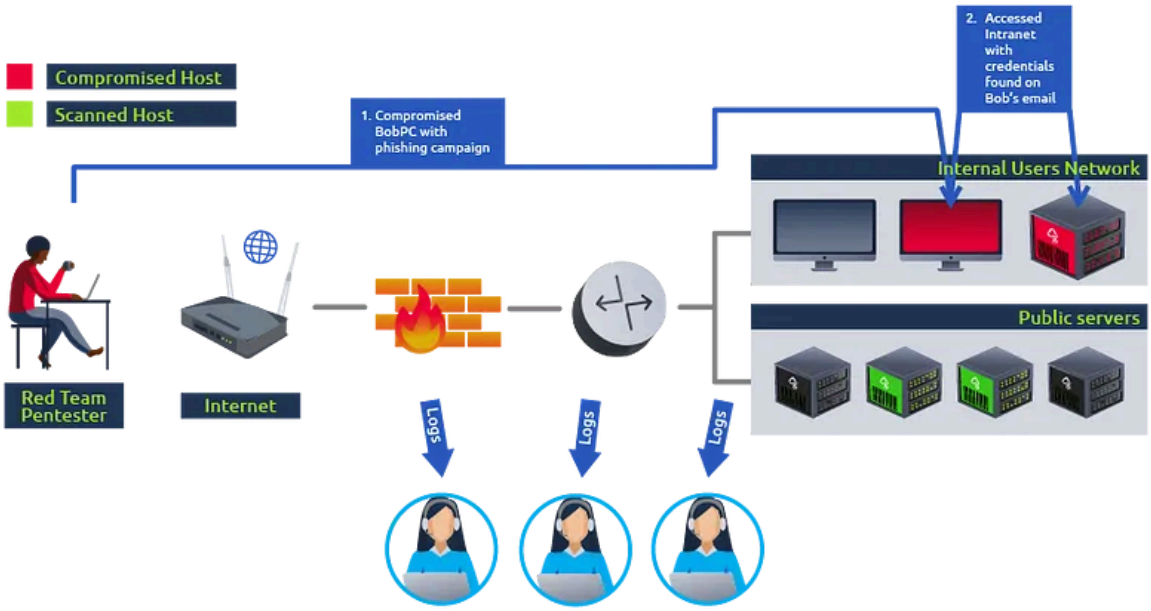
Task 3 : Red Team Engagements

To keep up with the emerging threats, red team engagements were designed to shift the focus from regular penetration tests into a process that allows us to clearly see our defensive team's capabilities at **detecting** and **responding** to a real threat actor. They don't replace traditional penetration tests, but complement them by focusing on detection and response rather than prevention.

Red teaming is a term borrowed from the military. In military exercises, a group would take the role of a red team to simulate attack techniques to test the reaction capabilities of a defending team, generally known as **blue team**, against known adversary strategies. Translated into the world of cybersecurity, red team engagements consist of emulating a real threat actor's **Tactics, Techniques and Procedures (TTPs)** so that we can measure how well our blue team responds to them and ultimately improve any security controls in place.

Every red team engagement will start by defining clear goals, often referenced as **crown jewels** or **flags**, ranging from compromising a given critical host to stealing some sensitive information from the target. Usually, the blue team won't be informed of such exercises to avoid introducing any biases in their analysis. The red team will do everything they can to achieve the goals while remaining undetected and evading any existing security mechanisms like firewalls, antivirus, EDR, IPS and others. Notice how on a red team engagement, not all of the hosts on a network will be checked for vulnerabilities. A real attacker would only need to find a single path to its goal and is not interested in performing noisy scans that the blue team could detect.

Taking the same network as before, on a red team engagement where the goal is to compromise the intranet server, we would plan for a way to reach our objective while interacting as little as possible with other hosts. Meanwhile, the blue team's capacity to detect and respond accordingly to the attack can be evaluated:



It is important to note that the final objective of such exercises should never be for the red team to "beat" the blue team, but rather simulate enough TTPs for the blue team to learn to react to a real ongoing threat adequately. If needed, they could tweak or add security controls that help to improve their detection capabilities.

Red team engagements also improve on regular penetration tests by considering several attack surfaces:

- **Technical Infrastructure:** Like in a regular penetration test, a red team will try to uncover technical vulnerabilities, with a much higher emphasis on stealth and evasion.
- **Social Engineering:** Targeting people through phishing campaigns, phone calls or social media to trick them into revealing information that should be private.
- **Physical Intrusion:** Using techniques like lockpicking, RFID cloning, exploiting weaknesses in electronic access control devices to access restricted areas of facilities.

Depending on the resources available, the red team exercise can be run in several ways:

- **Full Engagement:** Simulate an attacker's full workflow, from initial compromise until final goals have been achieved.
- **Assumed Breach:** Start by assuming the attacker has already gained control over some assets, and try to achieve the goals from there. As an example, the red team could receive access to some user's credentials or even a workstation in the internal network.
- **Table-top Exercise:** An over the table simulation where scenarios are discussed between the red and blue teams to evaluate how they would theoretically respond to certain threats. Ideal for situations where doing live simulations might be complicated.

Answer the questions below :

```
1. The goals of a red team engagement will often be referred to as flags or...
A. crown jewels

2. During a red team engagement, common methods used by attackers are emulated against the target. Such methods are usually
A. Tactics, techniques and procedures

3. The main objective of a red team engagement is to detect as many vulnerabilities in as many hosts as possible (Yay/Nay)
A. Nay
```

Task 4 : Teams and Functions of an Engagement

There are several factors and people involved within a red team engagement. Everyone will have their mindset and methodology to approach the engagement personnel; however, each engagement can be broken into three teams or cells. Below is a brief table illustrating each of the teams and a brief explanation of their responsibilities.

Team : Definition

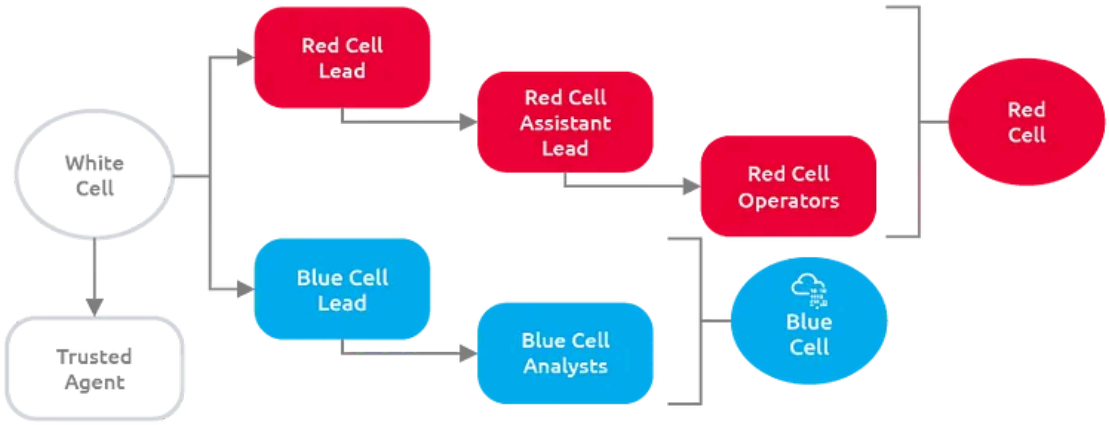
Red Cell : A red cell is the component that makes up the offensive portion of a red team engagement that simulates a given target's strategic and tactical responses.

Blue Cell : The blue cell is the opposite side of red. It includes all the components defending a target network. The blue cell is typically comprised of blue team members, defenders, internal staff, and an organisation's management.

White Cell : Serves as referee between red cell activities and blue cell responses during an engagement. Controls the engagement environment/network. Monitors adherence to the ROE. Coordinates activities required to achieve engagement goals. Correlates red cell activities with defensive actions. Ensures the engagement is conducted without bias to either side.

Definitions are sourced from redteam.guide.

These teams or cells can be broken down further into an engagement hierarchy.



Since this is a red team-oriented room, we will focus on the responsibilities of the red cell. Below is a table outlining the roles and responsibilities of members of the red team.

Role : Purpose

Red Team Lead : Plans and organises engagements at a high level — delegates, assistant lead, and operators engagement assignments.

Red Team Assistant : LeadAssists the team lead in overseeing engagement operations and operators. Can also assist in writing engagement plans and documentation if needed.

Red Team Operator : Executes assignments delegated by team leads. Interpret and analyse engagement plans from team leads.

As with most red team functions, each team and company will have its own structure and roles for each team member. The above table only acts as an example of the typical responsibilities of each role.

Answer the questions below :

```
1. What cell is responsible for the offensive operations of an engagement?
```

```
A. Red Cell

2. What cell is the trusted agent considered part of?
A. White Cell
```

Task 5 : Engagement Structure

A core function of the red team is adversary emulation. While not mandatory, it is commonly used to assess what a real adversary would do in an environment using their tools and methodologies. The red team can use various cyber kill chains to summarize and assess the steps and procedures of an engagement.

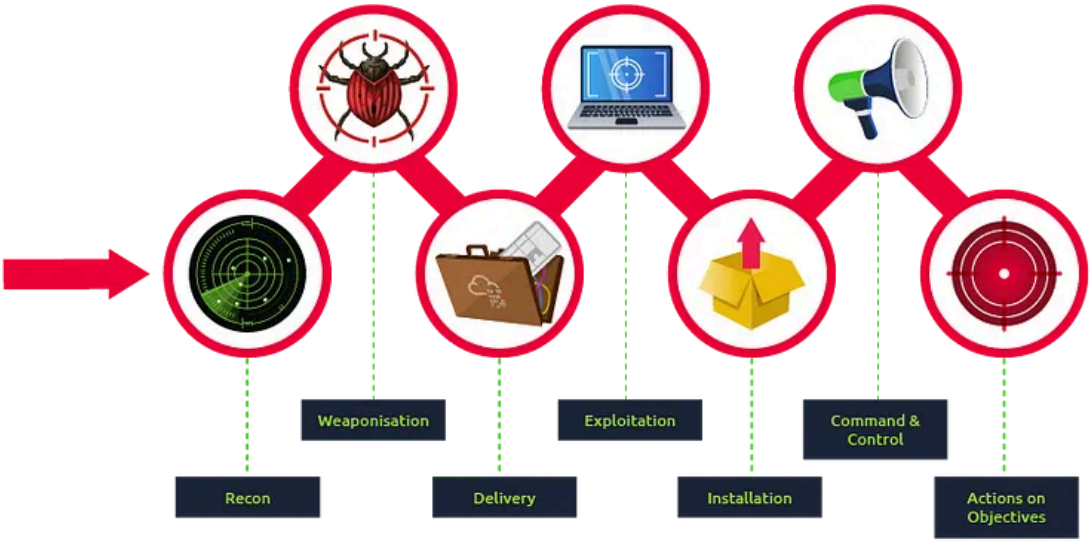
The blue team commonly uses cyber kill chains to map behaviors and break down an adversaries movement. The red team can adapt this idea to map adversary TTPs (**T**actics, **T**echniques, and **P**rocedures) to components of an engagement.

Many regulation and standardization bodies have released their cyber kill chain. Each kill chain follows roughly the same structure, with some going more in-depth or defining objectives differently. Below is a small list of standard cyber kill chains.

- Lockheed Martin Cyber Kill Chain
- Unified Kill Chain
- Varonis Cyber Kill Chain
- Active Directory Attack Cycle
- MITRE ATT&CK Framework

In this room, we will commonly reference the “Lockheed Martin Cyber Kill Chain.” It is a more standardized kill chain than others and is very commonly used among red and blue teams.

The Lockheed Martin kill chain focuses on a perimeter or external breach. Unlike other kill chains, it does not provide an in-depth breakdown of internal movement. You can think of this kill chain as a summary of all behaviors and operations present.



Components of the kill chain are broken down in the table below.

Technique	Purpose	Examples
Reconnaissance	Obtain information on the target	Harvesting emails, OSINT
Weaponization	Combine the objective with an exploit. Commonly results in a deliverable payload.	Exploit with backdoor, malicious office document
Delivery	How will the weaponized function be delivered to the target	Email, web, USB
Exploitation	Exploit the target's system to execute code	MS17-010, Zero-Logon, etc.
Installation	Install malware or other tooling	Mimikatz, Rubeus, etc.
Command & Control	Control the compromised asset from a remote central controller	Empire, Cobalt Strike, etc.
Actions on Objectives	Any end objectives: ransomware, data exfiltration, etc.	Conti, LockBit2.0, etc.

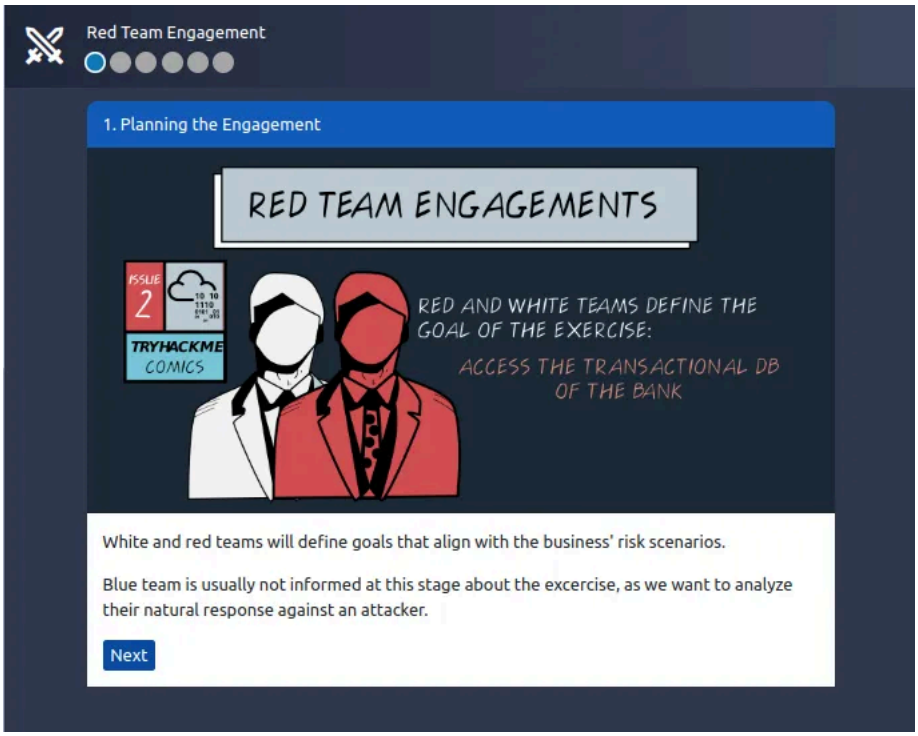
Answer the questions below :

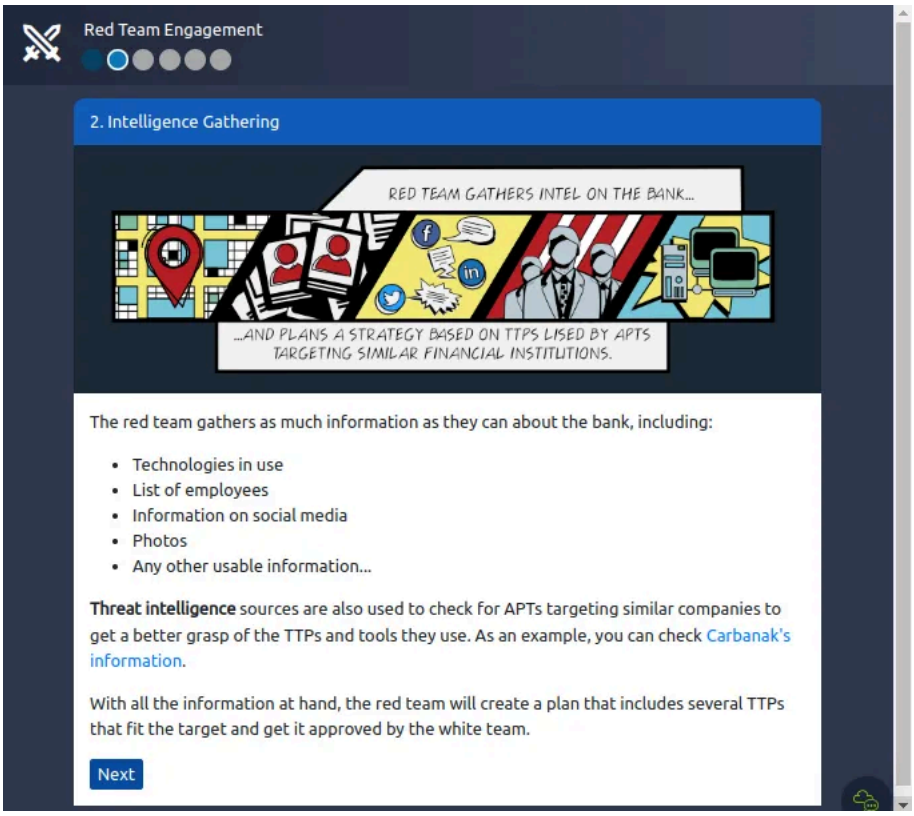
```
1. If an adversary deployed Mimikatz on a target machine, where would they be placed in the Lockheed Martin cyber kill chai
A. Installation

2. What technique's purpose is to exploit the target's system to execute code?
A. Exploitation
```

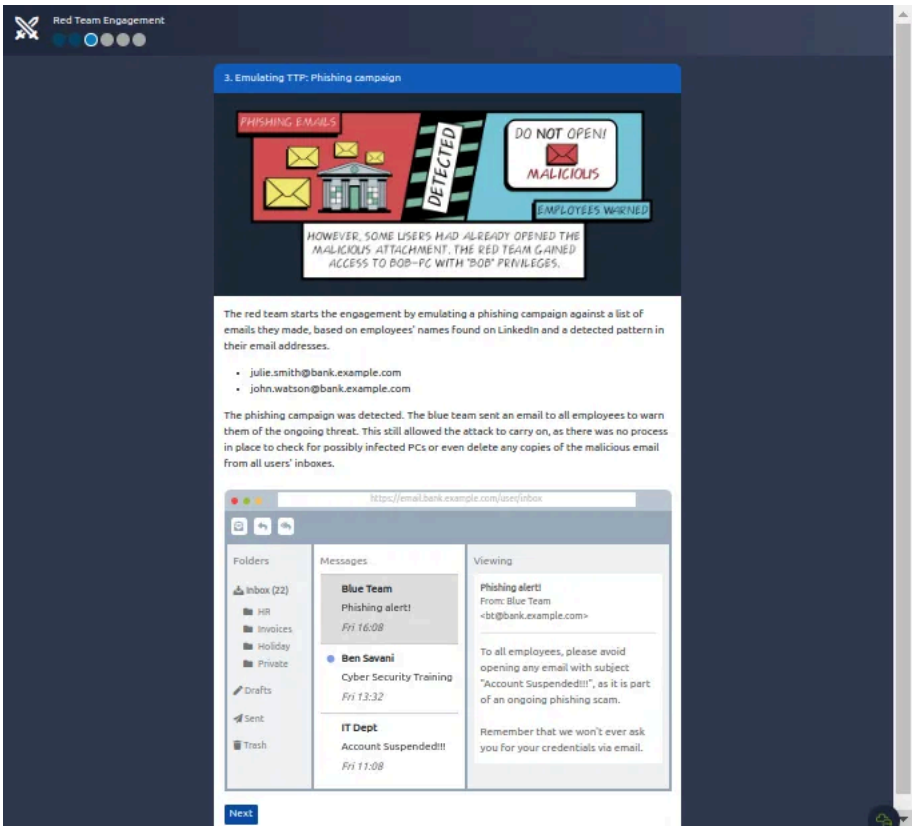
Task 6 : Overview of a Red Team Engagement

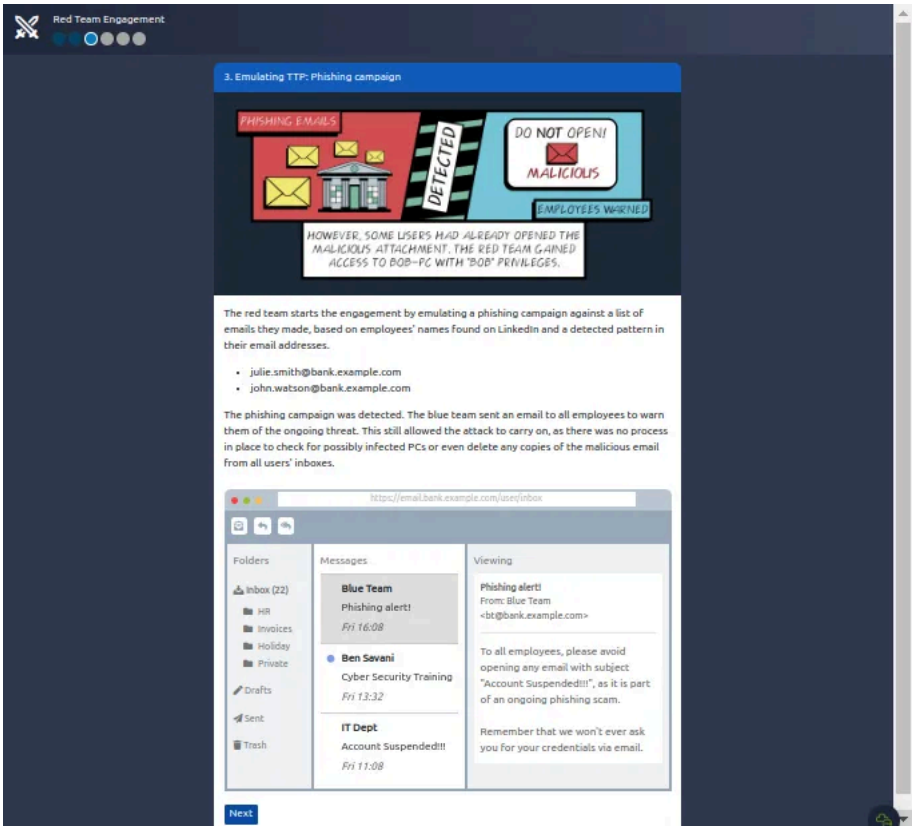
All the things we have discussed come together when performing a red team engagement. To better understand how the components and stakeholders interact, we will analyse a simplified engagement example. Navigate to the green “View Site” button to continue.

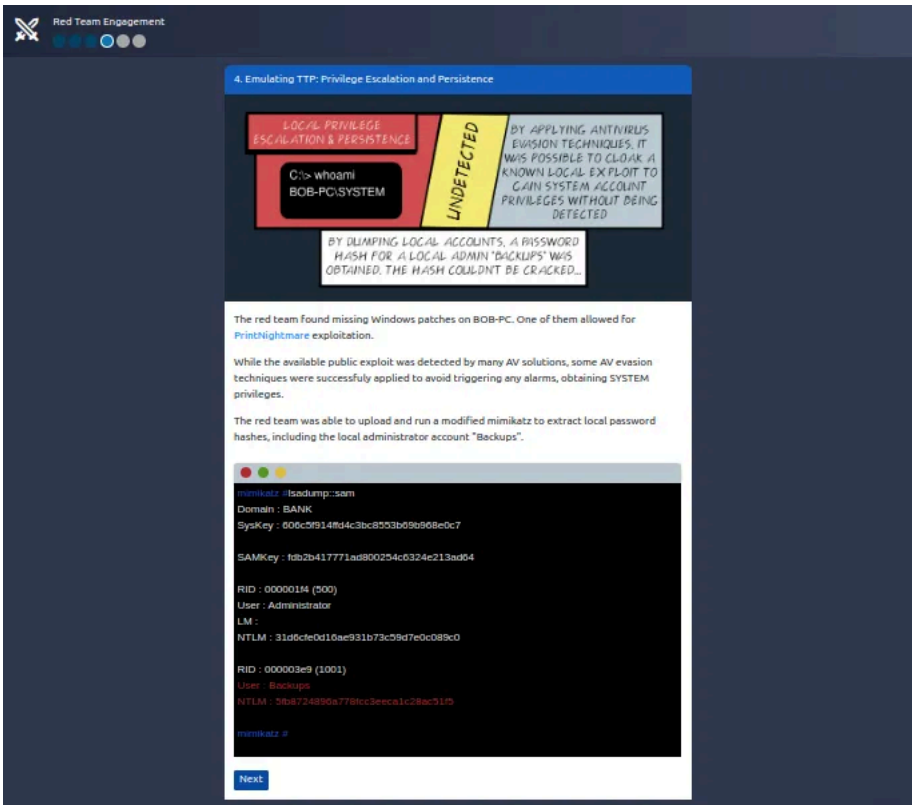
Notice how the Cyber Kill Chain naturally aligns with the exercise: We start with a **recon** phase where we gather as much intel as we can about our target, followed by **weaponization** and **delivery** by sending a phishing email with a malicious attachment, continued by **exploitation** and **installation** phases when using local exploits to elevate privileges on BOB-PC and then installing tools on compromised hosts to dump password hashes and perform lateral movement, to finish with **actions on objectives** where a connection to our target is finally made.

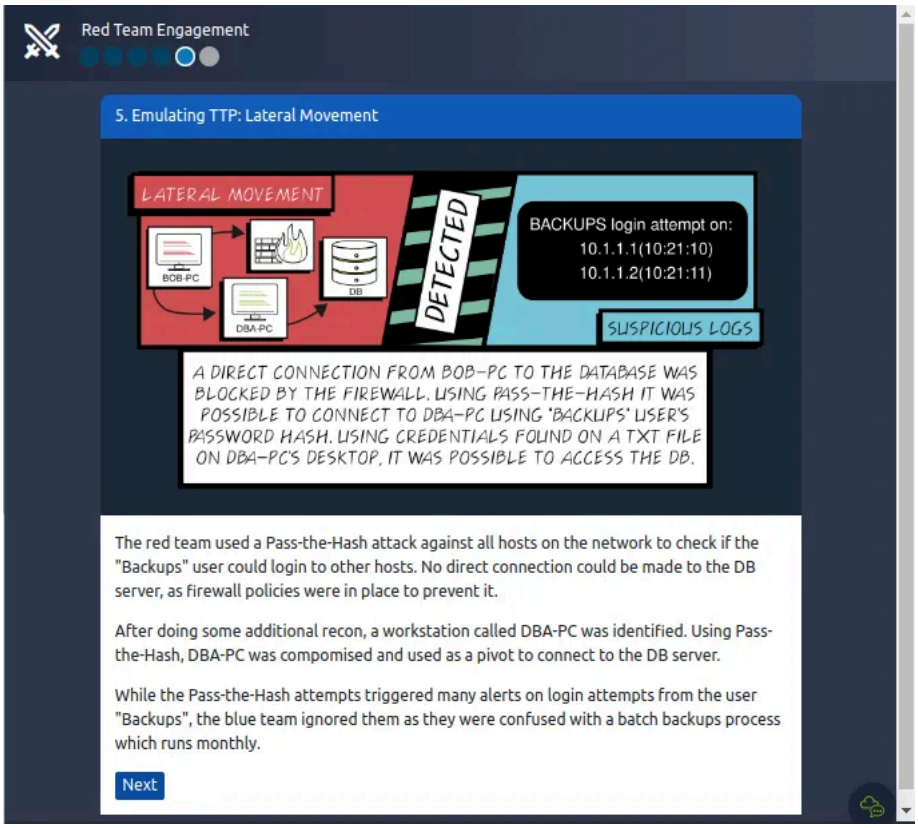

Red Team Engagement
1. Planning the Engagement
RED TEAM ENGAGEMENTS
ISSUE 2
TRYHACKME COMICS
RED AND WHITE TEAMS DEFINE THE GOAL OF THE EXERCISE:
ACCESS THE TRANSACTIONAL DB OF THE BANK
White and red teams will define goals that align with the business' risk scenarios.
Blue team is usually not informed at this stage about the excercise, as we want to analyze their natural response against an attacker.
Next

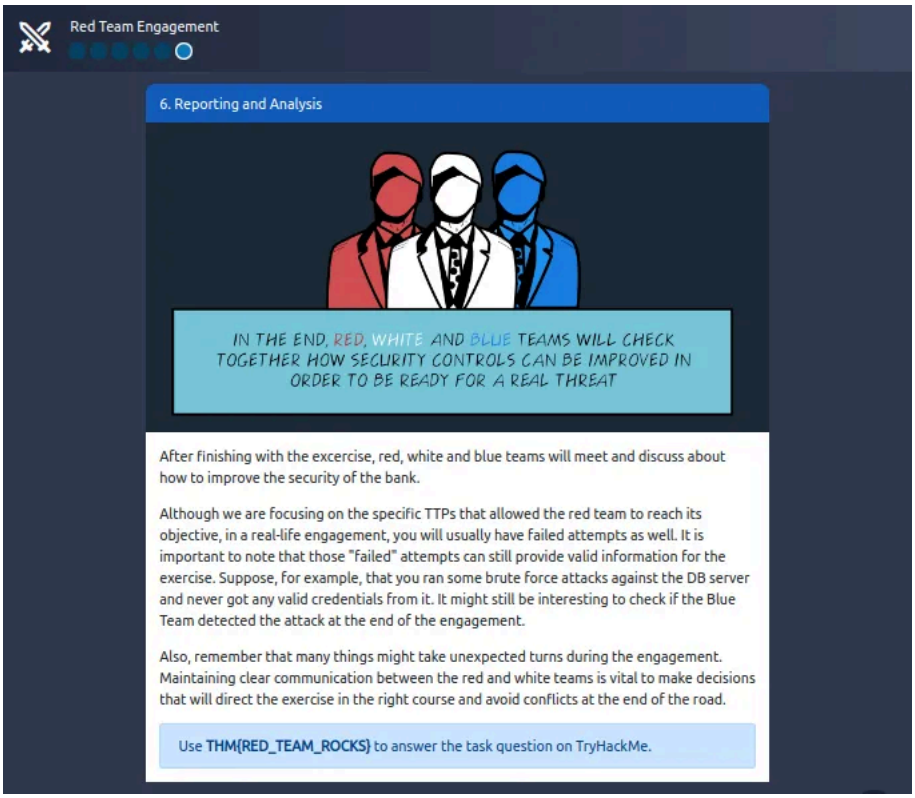

Red Team Engagement
2. Intelligence Gathering
RED TEAM GATHERS INTEL ON THE BANK...
...AND PLANS A STRATEGY BASED ON TTPS USED BY APTS TARGETING SIMILAR FINANCIAL INSTITUTIONS.
The red team gathers as much information as they can about the bank, including:
Technologies in use
List of employees
Information on social media
Photos
Any other usable information...
Threat intelligence sources are also used to check for APTs targeting similar companies to get a better grasp of the TTPs and tools they use. As an example, you can check Carbanak's information.
With all the information at hand, the red team will create a plan that includes several TTPs that fit the target and get it approved by the white team.
Next


Red Team Engagement
3. Emulating TTP: Phishing campaign
PHISHING EMAILS
DETECTED
DO NOT OPEN!
MALICIOUS
EMPLOYEES WARNED
HOWEVER, SOME USERS HAD ALREADY OPENED THE MALICIOUS ATTACHMENT. THE RED TEAM GAINED ACCESS TO BOB-PC WITH "BOB" PRIVILEGES.
The red team starts the engagement by emulating a phishing campaign against a list of emails they made, based on employees' names found on LinkedIn and a detected pattern in their email addresses.
julie.smith@bank.example.com
john.watson@bank.example.com
The phishing campaign was detected. The blue team sent an email to all employees to warn them of the ongoing threat. This still allowed the attack to carry on, as there was no process in place to check for possibly infected PCs or even delete any copies of the malicious email from all users' inboxes.
https://email.bank.example.com/user/inbox
Folders
Inbox (22)
HR
Invoices
Holiday
Private
Drafts
Sent
Trash
Messages
Blue Team
Phishing alert!
Fri 16:08
Ben Savani
Cyber Security Training
Fri 13:32
IT Dept
Account Suspended!!!
Fri 11:08
Viewing
Phishing alert!
From: Blue Team
<bt@bank.example.com>
To all employees, please avoid opening any email with subject "Account Suspended!!!", as it is part of an ongoing phishing scam.
Remember that we won't ever ask you for your credentials via email.
Next


Red Team Engagement
3. Emulating TTP: Phishing campaign
PHISHING EMAILS
DETECTED
DO NOT OPEN!
MALICIOUS
EMPLOYEES WARNED
HOWEVER, SOME USERS HAD ALREADY OPENED THE MALICIOUS ATTACHMENT. THE RED TEAM GAINED ACCESS TO BOB-PC WITH "BOB" PRIVILEGES.
The red team starts the engagement by emulating a phishing campaign against a list of emails they made, based on employees' names found on LinkedIn and a detected pattern in their email addresses.
julie.smith@bank.example.com
john.watson@bank.example.com
The phishing campaign was detected. The blue team sent an email to all employees to warn them of the ongoing threat. This still allowed the attack to carry on, as there was no process in place to check for possibly infected PCs or even delete any copies of the malicious email from all users' inboxes.
https://email.bank.example.com/user/inbox
Folders
Inbox (22)
HR
Invoices
Holiday
Private
Drafts
Sent
Trash
Messages
Blue Team
Phishing alert!
Fri 16:08
Ben Savani
Cyber Security Training
Fri 13:32
IT Dept
Account Suspended!!!
Fri 11:08
Viewing
Phishing alert!
From: Blue Team
<bt@bank.example.com>
To all employees, please avoid opening any email with subject "Account Suspended!!!", as it is part of an ongoing phishing scam.
Remember that we won't ever ask you for your credentials via email.
Next


Red Team Engagement
4. Emulating TTP: Privilege Escalation and Persistence
LOCAL PRIVILEGE ESCALATION & PERSISTENCE
C:\> whoami
BOB-PC\SYSTEM
UNDETECTED
BY APPLYING ANTIVIRUS EVASION TECHNIQUES, IT WAS POSSIBLE TO CLOAK A KNOWN LOCAL EXPLOIT TO GAIN SYSTEM ACCOUNT PRIVILEGES WITHOUT BEING DETECTED
BY DUMPING LOCAL ACCOUNTS, A PASSWORD HASH FOR A LOCAL ADMIN "BACKUPS" WAS OBTAINED. THE HASH COULDNT BE CRACKED...
The red team found missing Windows patches on BOB-PC. One of them allowed for PrintNightmare exploitation.
While the available public exploit was detected by many AV solutions, some AV evasion techniques were successfuly applied to avoid triggering any alarms, obtaining SYSTEM privileges.
The red team was able to upload and run a modified mimikatz to extract local password hashes, including the local administrator account "Backups".
mimikatz #lsadump::sam
Domain : BANK
SysKey : 606c5f914ffd4c3bc8553b69b968e0c7
SAMKey : fdb2b417771ad800254c6324e213ad64
RID : 00000114 (500)
User : Administrator
LM :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0
RID : 000003e9 (1001)
User : Backups
NTLM : 5fb8724896a778fcc3eeca1c28ac51f5
mimikatz #
Next


Red Team Engagement
5. Emulating TTP: Lateral Movement
LATERAL MOVEMENT
BOB-PC
DB
DBA-PC
DETECTED
BACKUPS login attempt on:
10.1.1.1(10:21:10)
10.1.1.2(10:21:11)
SUSPICIOUS LOGS
A DIRECT CONNECTION FROM BOB-PC TO THE DATABASE WAS BLOCKED BY THE FIREWALL. USING PASS-THE-HASH IT WAS POSSIBLE TO CONNECT TO DBA-PC USING "BACKUPS" USER'S PASSWORD HASH. USING CREDENTIALS FOUND ON A TXT FILE ON DBA-PC'S DESKTOP, IT WAS POSSIBLE TO ACCESS THE DB.
The red team used a Pass-the-Hash attack against all hosts on the network to check if the "Backups" user could login to other hosts. No direct connection could be made to the DB server, as firewall policies were in place to prevent it.
After doing some additional recon, a workstation called DBA-PC was identified. Using Pass-the-Hash, DBA-PC was compomised and used as a pivot to connect to the DB server.
While the Pass-the-Hash attempts triggered many alerts on login attempts from the user "Backups", the blue team ignored them as they were confused with a batch backups process which runs monthly.
Next



Answer the questions below :

```
1. Click the "View Site" button and follow the example engagement to get the flag
A. THM{RED_TEAM_ROCKS}
```

Task 7 : Conclusion

A simplified overview of Red Team Engagements has been provided in this room. The main concepts, components and stakeholders have been introduced to gain a first understanding of such exercises. In the rooms that follow you will learn all of the planning behind a real engagement, as well as a lot of cool techniques a real attacker would use along the way, including how to use threat intelligence to your advantage, evade security mechanisms present in any modern host, perform lateral movement and try to avoid detection at all costs.

Answer the questions below :

```
1. Read the above and continue learning!
A. No answer needed
```

Thankyou For Reading.

Tryhackme | Tryhackme Walkthrough | Infosec | Security | Cybersecurity

Follow

Published in InfoSec Write-ups

49K Followers · Last published 22 hours 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

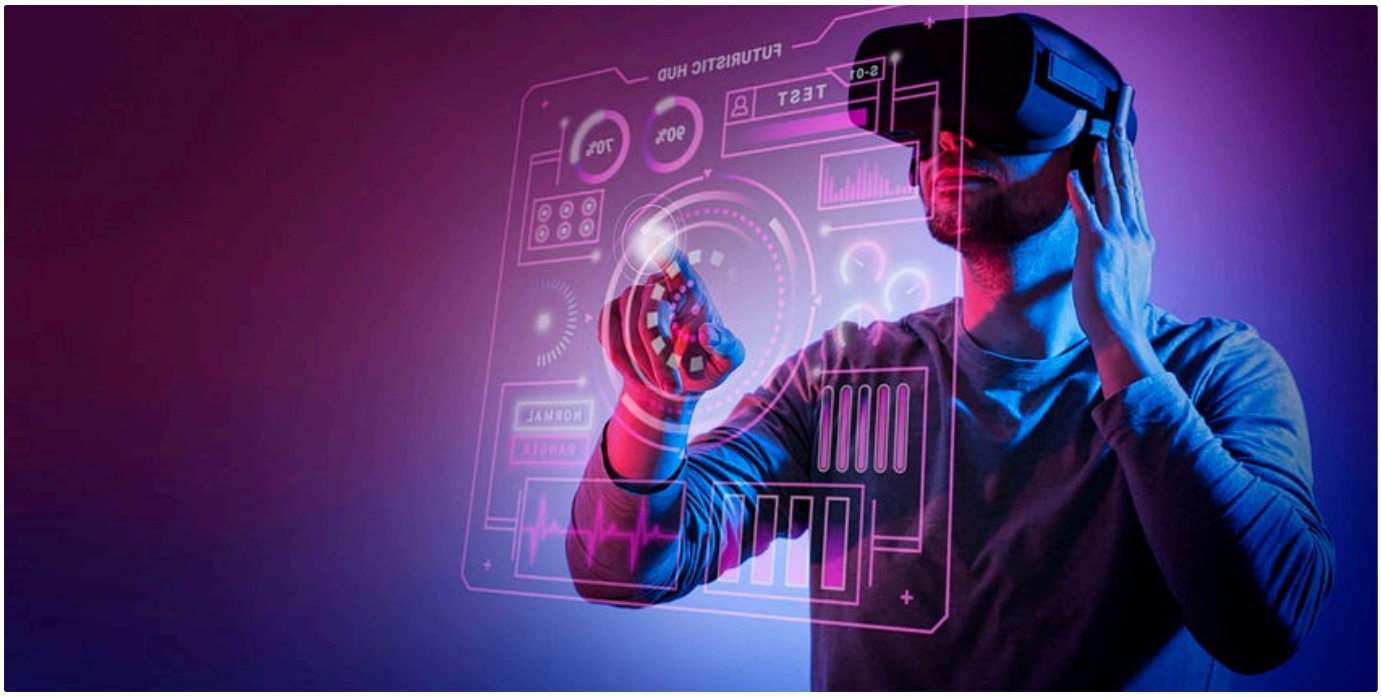
In InfoSec W... by Md Ami...
Outlook NTLM Leak | Tryhackme...
Mar 24, 2023

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

In InfoSec W... by Md Ami...
Red Team Engagements Tryhackme...
Mar 18, 2023

View list

More from Md Amiruddin and InfoSec Write-ups

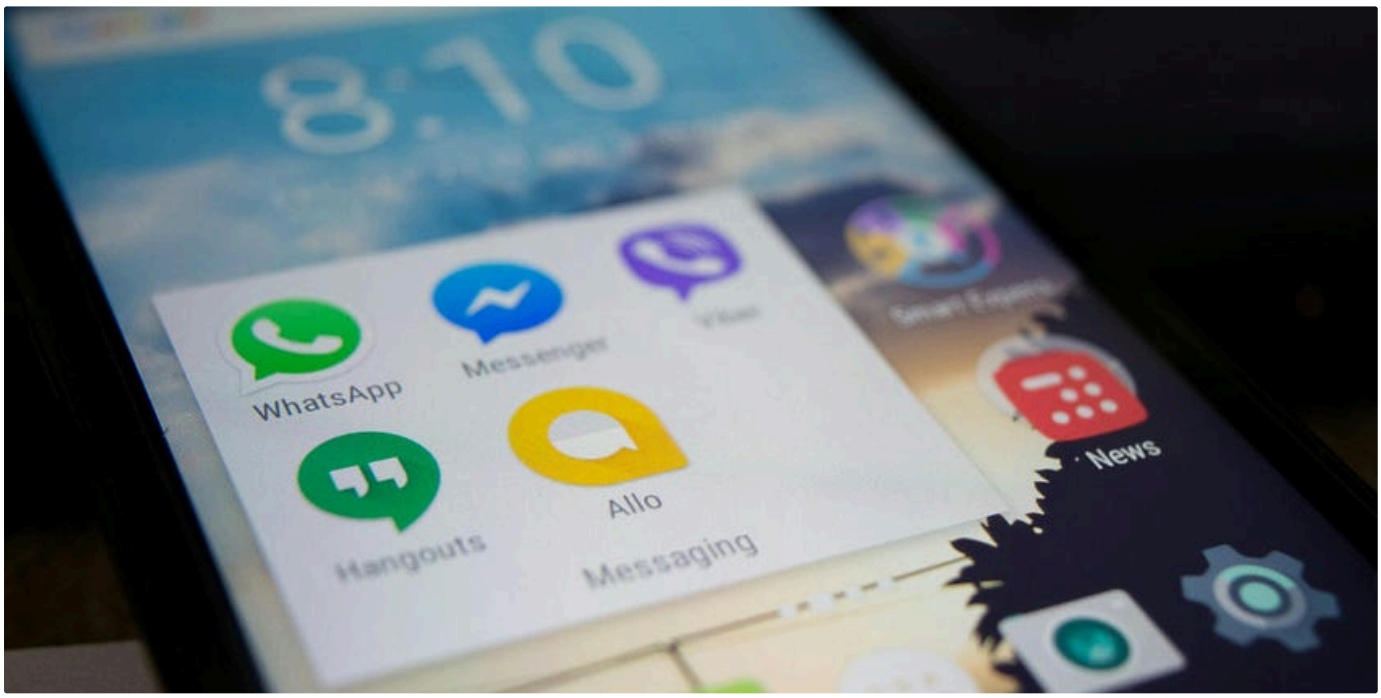


In InfoSec Write-ups by Md Amiruddin

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...

5d 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

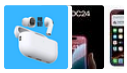
Angie

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

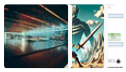
Lists



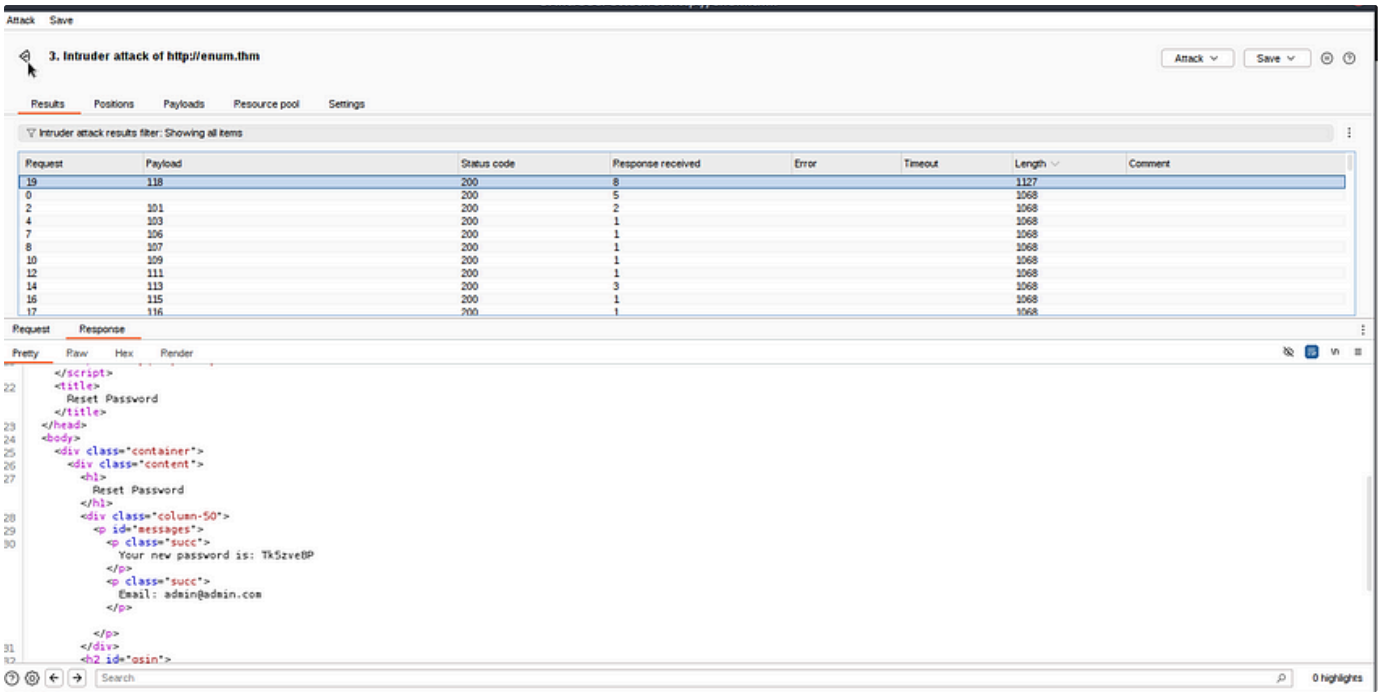
Tech & Tools
22 stories · 377 saves

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



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

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 13] Writeup with Answers | TryHackMe Walkthrough

It came without buffering! It came without lag!

Dec 13, 2024 868 1

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

See more recommendations