Red Team Fundamentals

Red Team Fundamentals

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

Introduction

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.

pentest and vuln assessment provide a good overview security posture of a company. but the are not like Real Attacks as real attacks are stealthy and more complex like bypassing the Security measures.

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

Vulnerability Assessment and Penetration Tests Limitations

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.

To summarize, Vulnerability Assessment focus on scanning as many hosts as possible detect as many Vulnerability as the Solution can and provide possible remediation.

They do not focus on exploitation.

Most of the work can be done with automated tools and performed by operators without requiring much technical knowledge.

Top Vulnerability Assessment Solutions are listed below

Nessus

Acunetix

Burp Suite

Nexpose

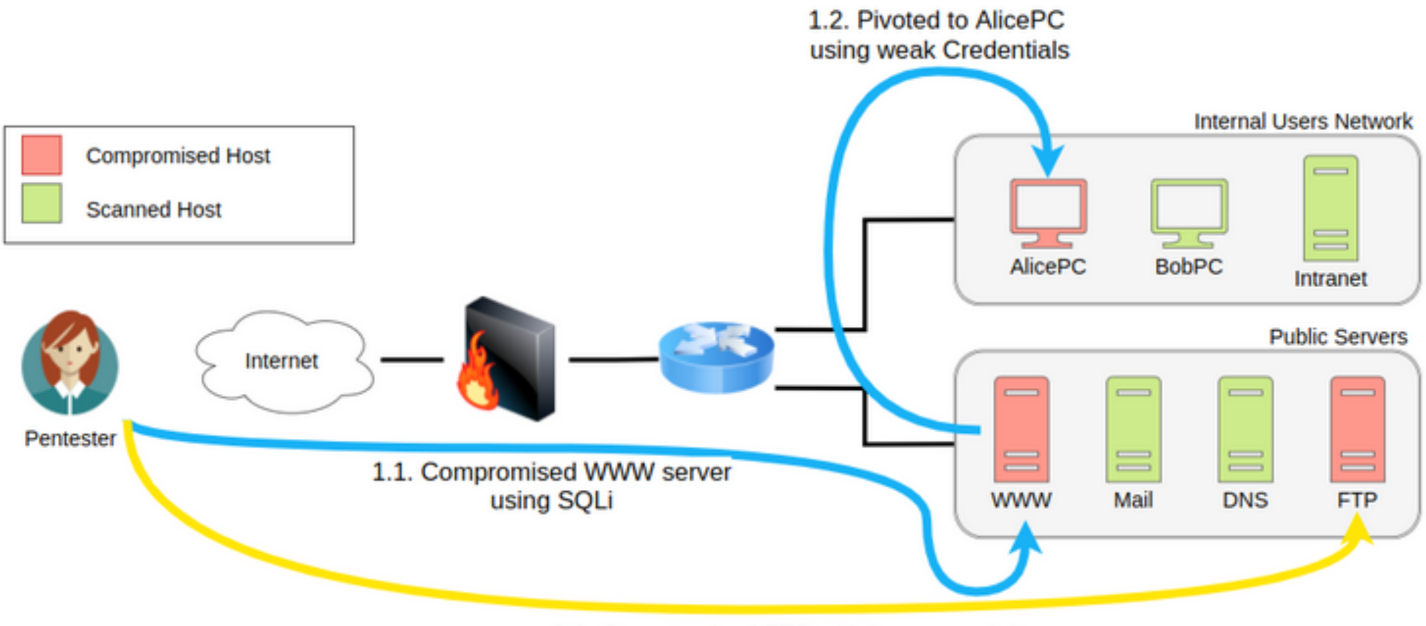
Nmap

Penetration Tests

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.

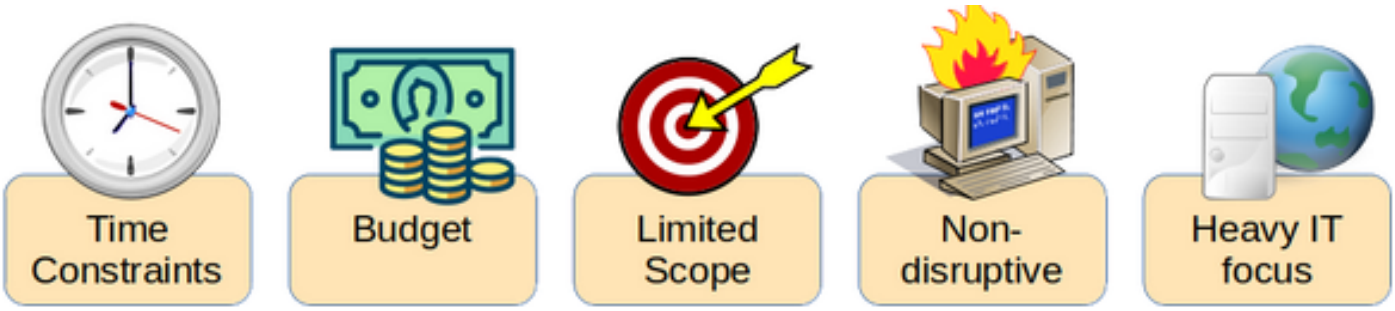
- Conduct **post-exploitation** tasks on any compromised host, allowing us to find if we can extract any helpful information from them or if we might use them to pivot to other hosts that were not previously accessible from where we stand.



Penetration 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

Pentest cover Vuln Detection and possible prevention, but because of the limitation in the pnetest scope will not let your company to prepare for a real attack.



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.

Advanced Persistent Threats (APT),

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 APT, could it detect when they get compromised, could they detect how long they are compromised.

What if APT used Social Engineering, or they used a Zero Day Vulnerability.

Red Team Engagements

Red Team Engagements

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 asĀ **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.

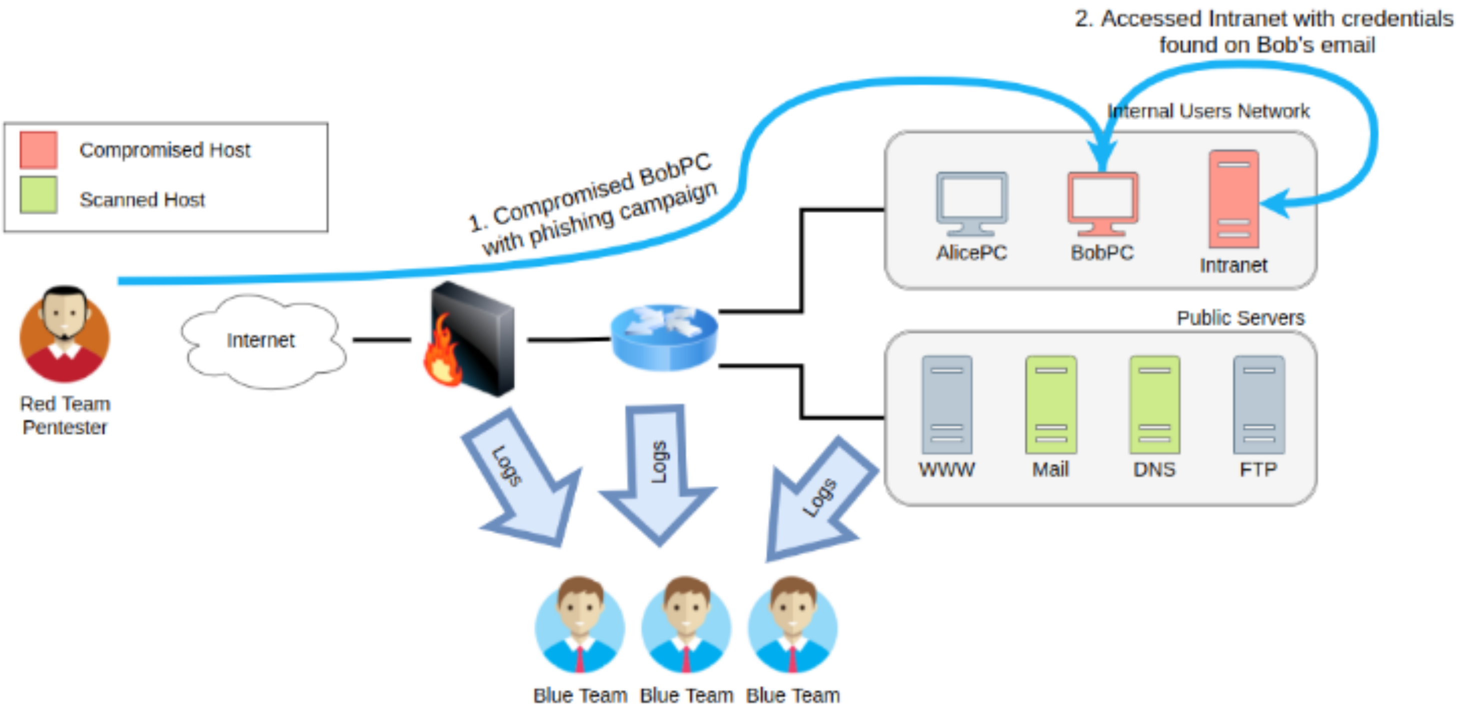
Every red team engagement will start by defining clear goals, often referenced as **crown jewels** or **flags**, ranging from compromising a given critical host to stealing some sensitive information from the target.

TTP

A tactic is the highest-level description of the behavior; techniques provide a more detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed description of the behavior in the context of a technique.

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.



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.

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

- **Technical Infrastructure:**┬áLike 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.

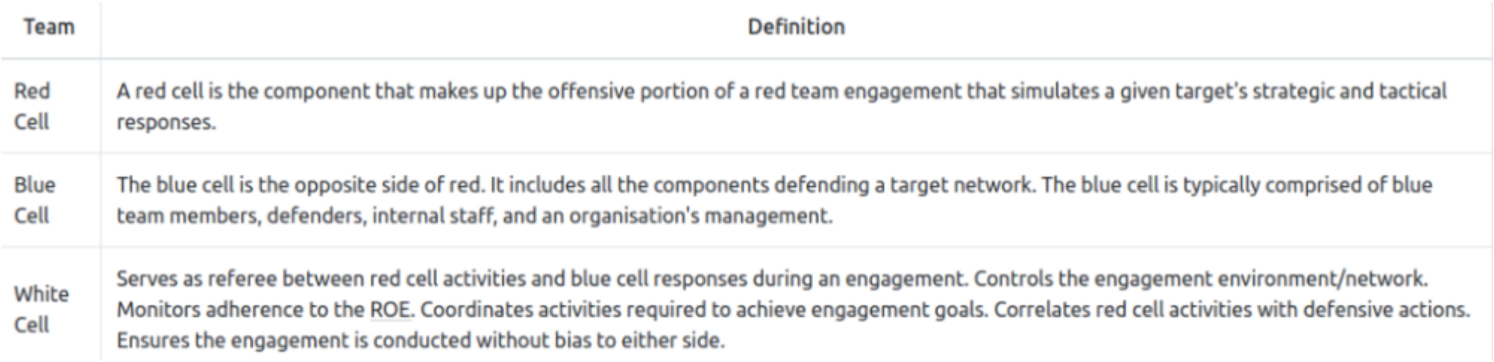
- **Assumed Breach:** Start by assuming the attacker has already gained control over some assets, and try to achieve the goals from there. As an example, the red team could receive access to some user's credentials or even a workstation in the internal network.

- **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.

Teams and Functions of an Engagement

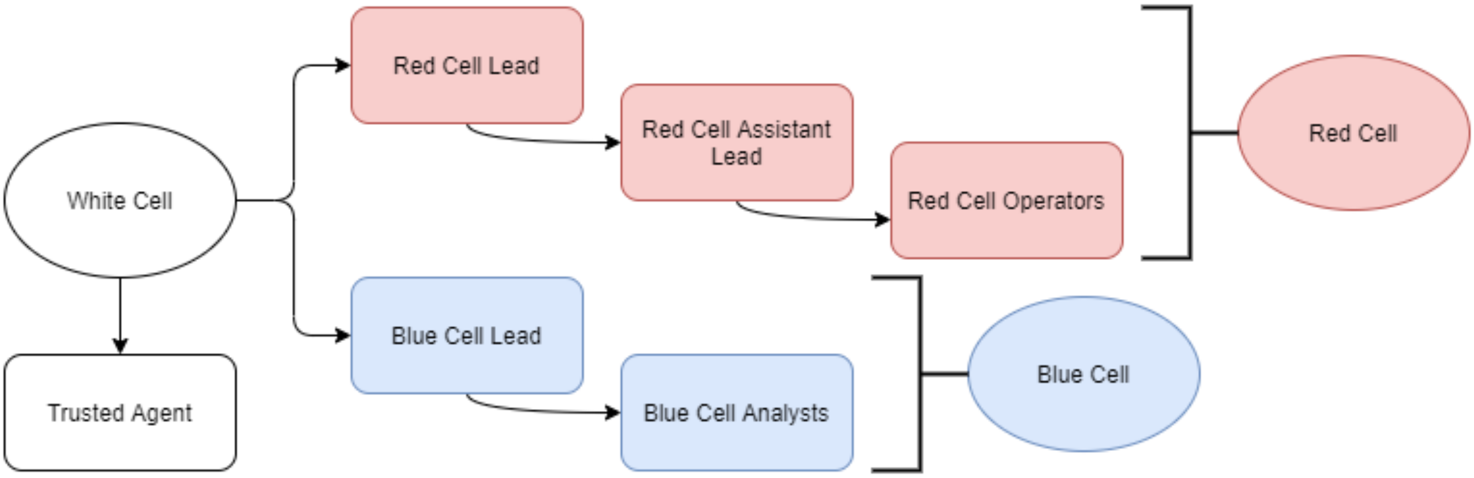
Teams and Functions of an Engagement

Engagement can be broken into three teams or cells.

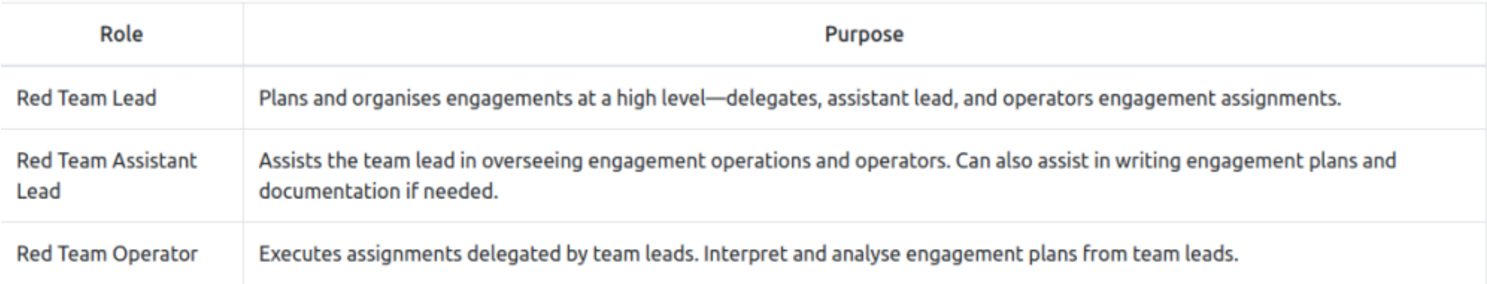


Team	Definition
Red Cell	A red cell is the component that makes up the offensive portion of a red team engagement that simulates a given target's strategic and tactical responses.
Blue Cell	The blue cell is the opposite side of red. It includes all the components defending a target network. The blue 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.

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



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 Lead	Assists 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.

Engagement Structure

Engagement Structure

Red Team

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.

Blue Team

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.

Cyber kill chain

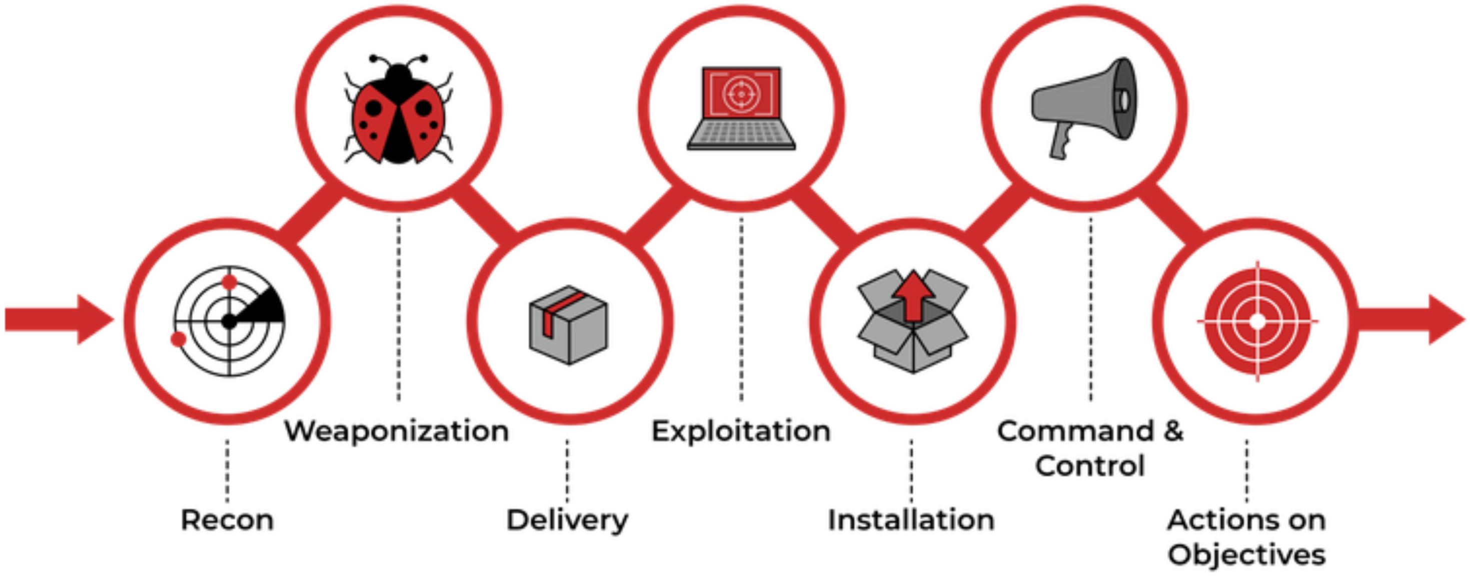
Many regulation and standardization bodies have released their cyber kill chain.

Below is a small list of standard cyber kill chains.

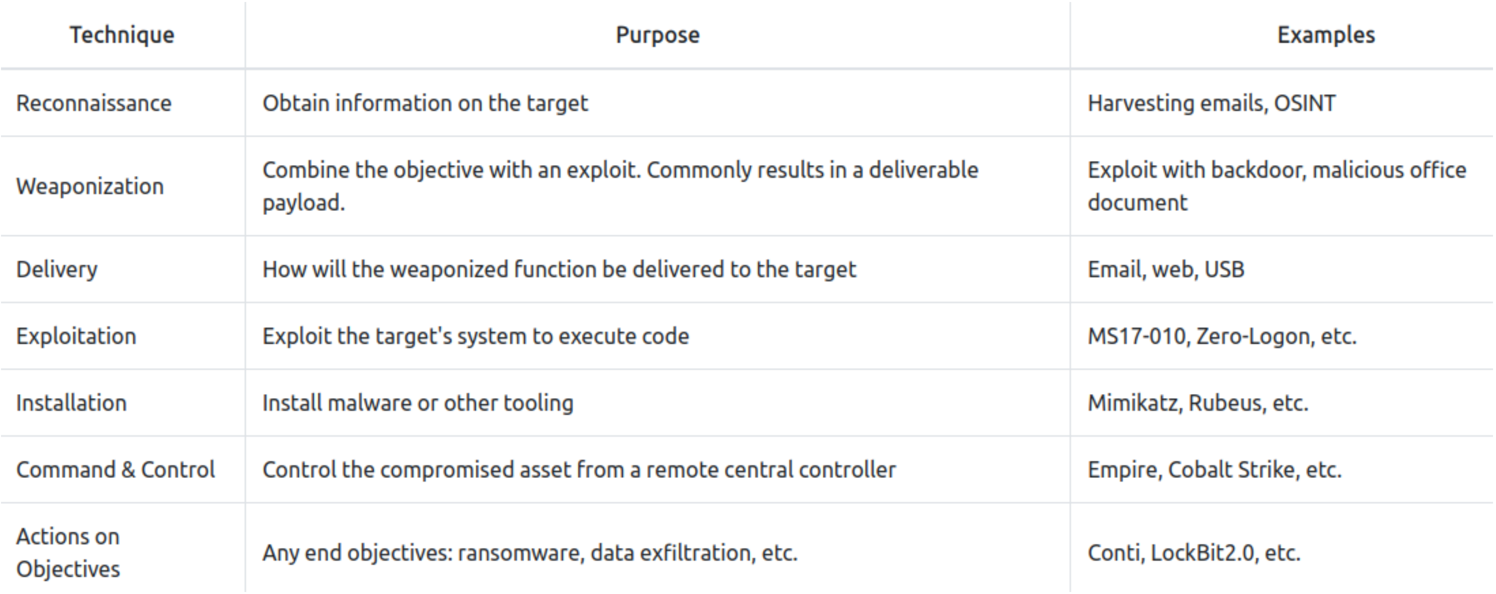
- Lockheed Martin Cyber Kill Chain
- Unified Kill Chain
- Varonis Cyber Kill Chain
- Active Directory Attack Cycle
- MITRE ATT&CK Framework

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, does not go in-depth breakdown of internal movement, you may think that 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.

Overview of a Red Team Engagement

1. Planning the Engagement

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.

2. Intelligence Gathering

The red team gathers as much information as they can about the target. like:

- Technologies in use
- List of employees
- Information on social media
- Photos
- Any other usable 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.

Note:
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.

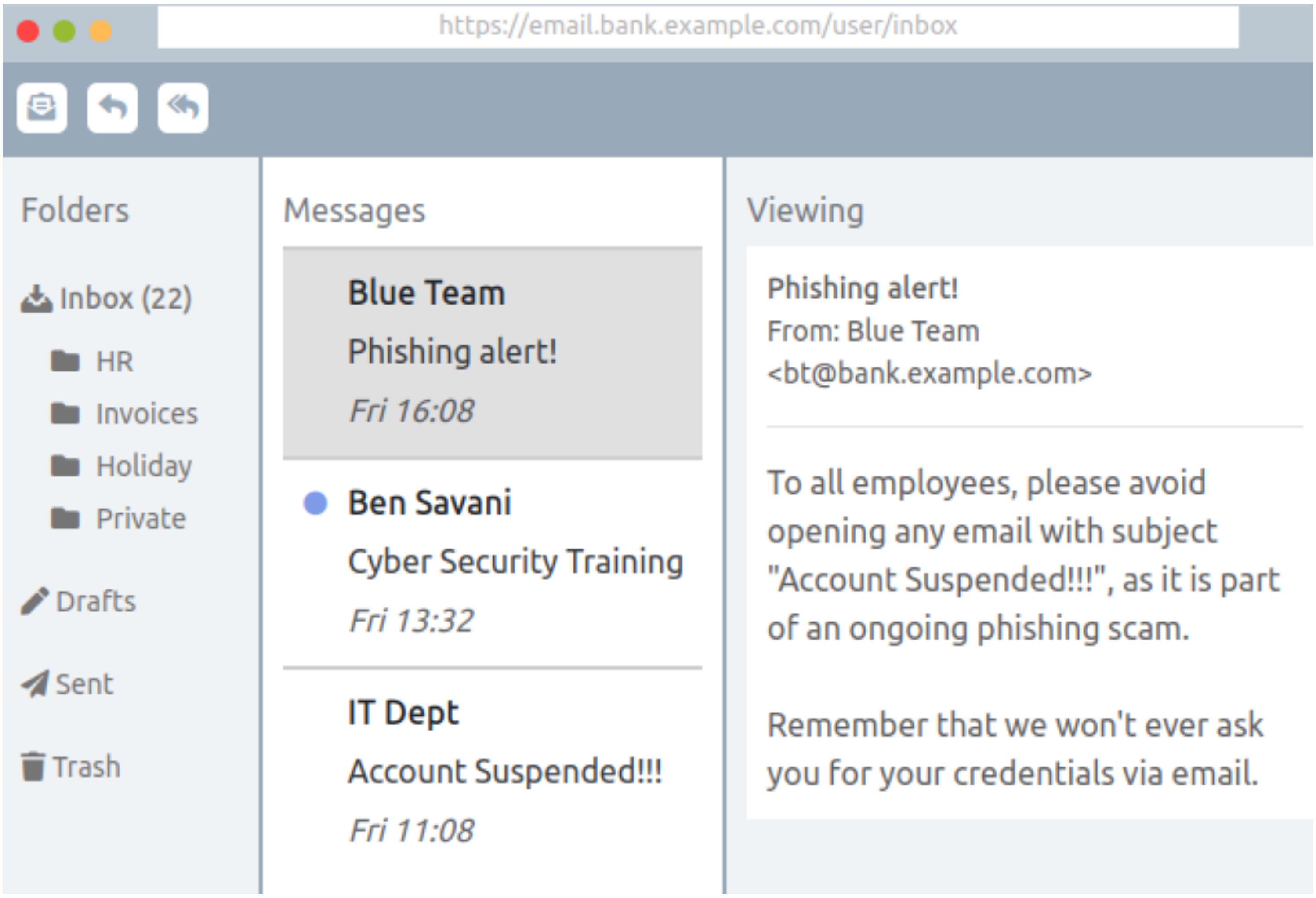
3. Emulating TTP: Phishing campaign

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.



Blue Team
Phishing alert!
Fri 16:08

Ben Savani
Cyber Security Training
Fri 13:32

IT Dept
Account Suspended!!!
Fri 11:08

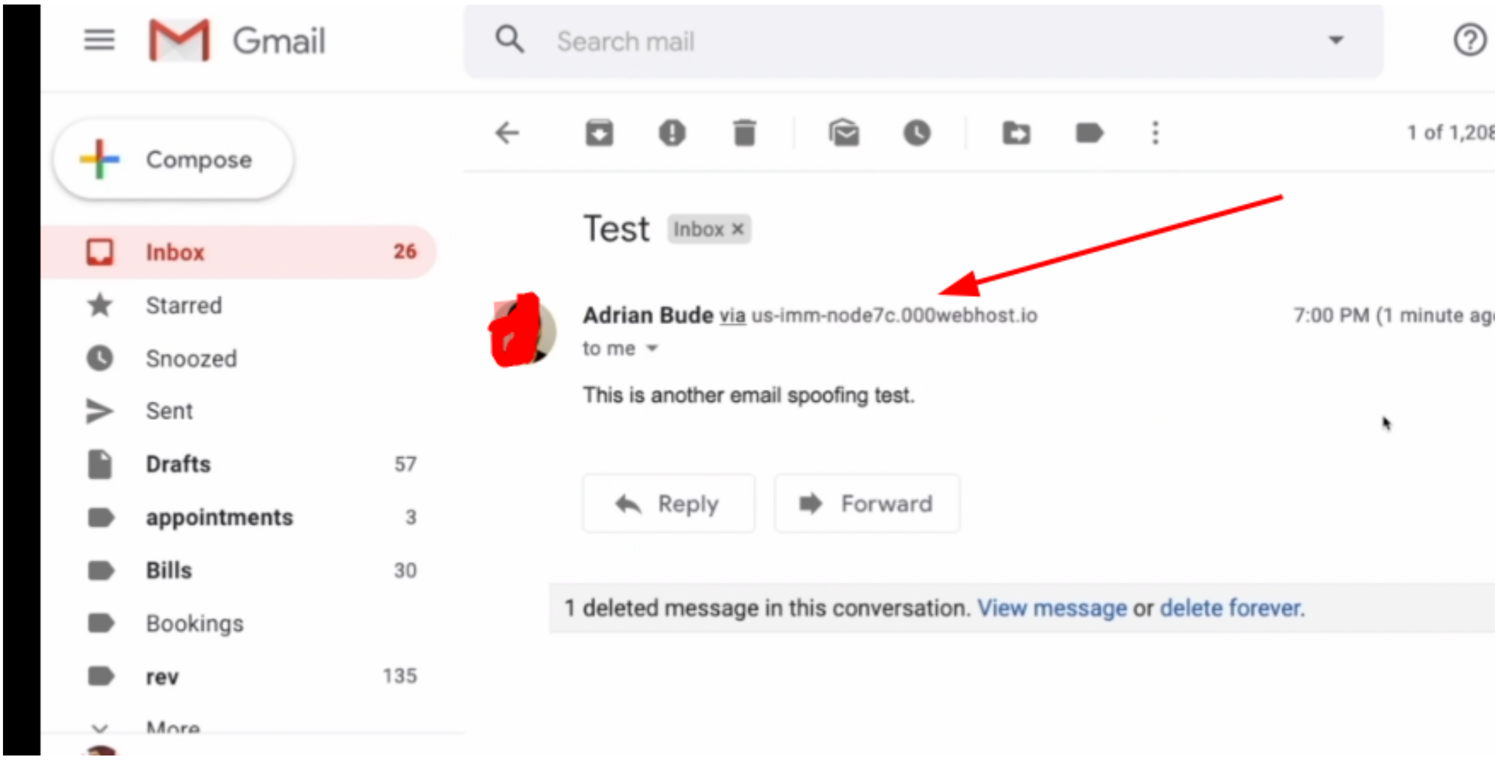
Phishing alert!
From: Blue Team <bt@bank.example.com>

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.

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.

In Real Life a spoofed email would look like this



Test Inbox ×

[redacted] Adrian Bude via us-imm-node7c.000webhost.io 7:00 PM (1 minute ag
to me

This is another email spoofing test.

1 deleted message in this conversation. View message or delete forever.

4. Emulating TTP: Privilege Escalation and Persistence

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 successfully 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".

5. Emulating TTP: Lateral Movement

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.

6. Reporting and Analysis

After finishing with the excercise, red, white and blue teams will meet and discuss about how to improve the security of the bank.

Although we are focusing on the specific TTPs that allowed the red team to reach its objective, in a real-life engagement, you will usually have failed attempts as well. It is important to note that those "failed" attempts can still provide valid information for the exercise. Suppose, for example, that you ran some brute force attacks against the DB server and never got any valid credentials from it. It might still be interesting to check if the Blue Team detected the attack at the end of the engagement.

Also, remember that many things might take unexpected turns during the engagement. Maintaining clear communication between the red and white teams is vital to make decisions that will direct the exercise in the right course and avoid conflicts at the end of the road.

Conclusion

Conclusion

A simplified overview of Red Team Engagements has been provided in this room.

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.