International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Red Team Operations and Common Attack Vectors

Bogdan Barchuk *

Independent Resaercher.

International Journal of Science and Research Archive, 2023, 10(01), 1209-1221

Publication history: Received on 18 July 2023; revised on 20 September 2023; accepted on 25 September 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.10.1.0704

Abstract

By using red team operations, a company can assess its cybersecurity and make necessary improvements by conducting simulated attacks. Among the common approaches they use are scanning networks, using flaws to break in, releasing malware, launching phishing scams, and attacking cloud servers. The aim is to spot security flaws ahead of malicious attacks, so companies can understand how to better protect themselves. This research describes how to approach red team scenarios, including the usual stages of scanning, exploiting systems, acting after gaining access, and maintaining that access. It adds that some of the main approaches and resources needed are gathering credentials, moving across a system, and making it more difficult to track the intruder. Furthermore, the study investigates how attackers make use of stolen usernames, scam victims, and insecure cloud settings. Studying these vectors and methods gives security teams the ability to recognize and handle risks ahead of time. Here, you will find clear directions for red teaming that helps security experts and ethical hackers to carry out real-word scenarios to boost an organization's ability to tackle new risks.

Keywords: Red Teaming; Phishing Attacks; Cloud Security; Payload Delivery; Privilege Escalation; Defense Evasion

1. Introduction

Cybersecurity experts use red teaming to create simulated adversarial attacks to learn how well an organization is prepared. It gives an active method to point out weaknesses, evaluate current defenses, and increase response to any incident. It is important to include red teaming because it acts like real attackers and allows security teams to identify and address risks ahead of any actual breaches. By doing this, companies can find weaknesses in their security systems that normal defenses might not detect.

By using ethical methods, offensive security testing supports red teaming and permits attacks to happen only in ways permitted by the team. It relies on a certain approach designed to find weaknesses, ensuring little disturbance to daily activities. Penetration testing, social engineering, and looking for vulnerabilities are some of the methods ethical hackers use to test and report on system strength to stakeholders. It helps connect defensive features to the way hackers attack, which provides useful ideas for always improving the model.

Recent analysis demonstrates that attack strategies are evolving and becoming more advanced, with penetration testing strategies being one of the main examples (Aibekova & Selvarajah, 2022). Committed teams have also developed regulatory strategies, which make it simple to hunt for and exploit online security loopholes (Cuzme-Rodríguez et al., 2018). As a result, red teaming and ethical offensive security testing are recognized as vital parts of up-to-date ways to secure networks and systems.

* Corresponding author: Bogdan Barchuk

1.1. Overview

Red team operations are built around important phases meant to represent the conduct of an adversary. Usually, penetrating networks begins with gathering information, followed by infecting computers with tools, sending the compromise to targets, taking advantage of the attack, placing controls on the system, and taking actions on the intended targets. By taking a phased approach, red teams can simulate real-world attacks, giving companies an understanding of how an advanced attacker could get inside and move around their network. By repeating these phases, the process ensures that changes are made to meet the ongoing challenges in threat landscapes.

Usually, the first stage of an attack involves attackers finding out as much as they can about the target's organization and its people. This is followed by preparing and accessing software that checks for and utilizes vulnerable areas of networks. When they have gained initial access to the system, attackers try to stay in it smoothly, increase their privileges, and travel further to produce the biggest outcome. To achieve their goals, the opponent will try to exfiltrate data or disrupt essential services. It is necessary to know about the lifecycle when planning and creating defense strategies.

Researchers now indicate that red teaming is expanding into AI testing, with phase-by-phase analytical steps to discover any uncovered weaknesses in AI systems (Perez et al., 2022). Moreover, good critical thinking helps red teams respond to changes in the operation context and act strategically through the entire engagement (Constantinianu, 2020). Overall, this highlights that red team tasks are carefully planned and ensure the organization's overall security.

1.2. Problem Statement

Dealing with today's advanced attacks is difficult for most organizations. Attackers often use new tactics and methods that adapt over time and can get around standard forms of security. Defenders must respond in real time and adapt to the many forms of attack, such as malware made for a specific victim, fishing for confidential information with emails, and using cloud services without permission. Many organizations find it difficult to prepare for every possible type of threat. Moreover, it is difficult for security teams to spot significant weaknesses and assess defenses without well-planned and accurate simulations. It slows down the process of creating useful response and mitigation plans. There is a strong need for consistent simulated red team operations to handle the growing problem of multiple threat behaviors. Because of such methods, organizations can judge their potential survival, improve security equipment, and tighten their security plans. Using a well-organized approach to red teaming is needed to reach a balance between the capabilities of current defenses and those used by attackers.

1.3. Objectives

The main focus of this study is to list common ways attacks are carried out in red team operations for the benefit of security experts. The research examines commonly-used approaches such as scanning computer networks, spreading malware, phishing, and exploiting the cloud. This explains the risks and tells how to defend against them. Besides, the study proposes a well-defined framework and lists essential steps and devices that enable red team members to conduct simulations resembling true threats. It aims to go through every stage of an attack and keep security high throughout the process. In addition, these methods are evaluated by running case studies that display how red team exercises actually work and what results are produced. The main goal is to progress in offensive security so that businesses can get prepared and respond effectively to cyber threats.

1.4. Scope and Significance

This study focuses on main attack vectors related to red team activities nowadays, such as network attacks, distributing malware, phishing campaigns, and attacks on cloud services. The methods listed in these vectors are the most common and significant ways threats affect the security of organizations. Because it focuses on those factors, the study offers guidance for use in numerous industries and settings. This work can boost a system's security, as it uncovers potential weaknesses ahead of others' attempts. With this information, security teams can see possible risks coming and create better systems to prevent and detect them. It also increases everyone's understanding of security risks, prompting them to act wisely. The approach ensures that red team exercises are useful and effective at dealing with new dangers in today's threat environment.

2. Literature review

2.1. Cycle of a Red Team Attack and the Tools They Use

Red team work uses a clear process to mimic real attacks and effectively test the security of a company. As a rule, this lifecycle is made up of three essential phases. reconnaissance, exploitation, and persistence. Red teams perform reconnaissance to learn about the target network's defense system, find out where they might access it, and search for network weaknesses. It is important during this phase to develop a step-by-step plan designed for the selected target.

During the exploitation phase, the attacker takes advantage of the vulnerabilities to gain access or handle the systems without permission. Techniques can involve using various software errors, misconfigured settings, or poor passwords. At this step, the organization identifies whether its security systems are working well in catching and preventing security breaches. As soon as the attackers gain access, they start the persistence phase where they try to hide and keep control for a longer time. It refers to creating backdoors, raising one's privileges, and moving to other vulnerable systems.

To achieve success in these steps, red teams rely on various up-to-date security tools. Rustscan and Masscan are used for their quick results in viewing network details of large IP ranges. For the purpose of exploitation and attacking, Metasploit, Cobalt Strike, and Covenant are the most commonly used frameworks. With Metasploit, it is possible to design and run exploits, while Cobalt Strike gives control over malware and supports various social engineering activities. Due to its ability to manage and organize payloads, Covenant is suitable for all kinds of environments.

Studies now show that red team emulation tools are useful for simulating the moves of clever attackers. In his paper, Holm includes Lore, a tool that simulates attacks to improve the realism and effectiveness of all types of red teams. In the same vein, Elgh (2022) looks at several emulation environments and highlights the importance of choosing suitable tools to ensure cyber attack actions are well tested. All in all, it emphasizes that successful red team activities require a thorough reporting process and winning tools.

2.2. Network and Vulnerability Scanning

Carrying out network and vulnerability scans is necessary at the start of red team operations to uncover weaknesses in various systems. Red teams perform effective scanning to find the structure of the network, see what is running and active, and find any weaknesses that could be exploited further. Many IT experts conduct thorough assessments with the help of Nessus, Acunetix, and Burp Suite.

With Nessus's many plugins, it scans for known flaws present in different systems and services automatically. Acunetix is focused on web app security, helping to spot issues like SQL injection, cross-site scripting, and failing authentication. Burp Suite works together with these tools by offering an interactive area for discovering web security problems and using them to compromise a system.

Part of vulnerability scanning involves picking the right attack tools and focusing them on the most appropriate platforms. As Image 1 shows, red teams usually prefer certain operating systems for their trojan or malware, selecting Windows since it is used by the largest number of organizations. Understanding what platform you are attacking helps attackers design payloads that best suit and can attack that platform.

Sometimes, red teams use Masscan and Rustscan to scan for open ports quickly and then use vulnerability scanners to look for chinks in the system's services in more detail. Once a weakness is found, hackers can use Metasploit or Cobalt Strike to turn it into a way to access the system.

The phase's achievements are determined by proper scanning and accurately identifying vulnerabilities to improve exploitation procedures. Platform-aware payloads together with advanced scanning enable red teams to show, through simulations, where the defenses can be further improved.

Figure 1 Platform Selection for Trojan Attack Payloads – Demonstrates targeting options available during network exploitation to tailor payload delivery based on the victim's operating system

2.3. Malware and Payload Delivery Mechanisms

In the red team's process, red team members deploy their carefully designed malware to attack the target. Red teams depend on tools such as Metasploit, Cobalt Strike, and Empire to construct diverse and covert agents for any kind of attack. Attackers may use executable files, Office documents with macros, PDFs, or compressed archives to ensure greater chances of infection.

Image 2 shows some ways in which the payload is wrapped to avoid being detected and more easily get through to its destination. With the Not Packed selection, you give the target a raw .exe file that is installed as soon as it is opened. Filtering out some email filters can be done by compressing the payloads into PKZIP or GZIP archives, which must first be unpacked by users. By creating a payload within a Microsoft Excel file using VBA macros, hackers can fool users into allowing their computers to execute harmful code. In a similar way, vulnerable versions of Adobe Reader can be infected by malicious PDFs uploaded on Adobe's platform. Another approach called Infected Binary tricks participants by attaching infected legitimate files to their emails.

Attackers can design the payload based on factors such as the network environment and the level of security in place. Choosing port 443, 80, or 53 for payload communication can help the traffic go unnoticed by network monitoring. Furthermore, through obfuscation and encoding, it becomes more possible to get through antivirus and intrusion detection systems.

Using different payloads and ways to spread them, red teams set up situations that make it look like attacks have taken place, testing how efficiently the organization can find and deal with malware. Taking various steps is necessary to discover where the endpoint and user security might be flawed.

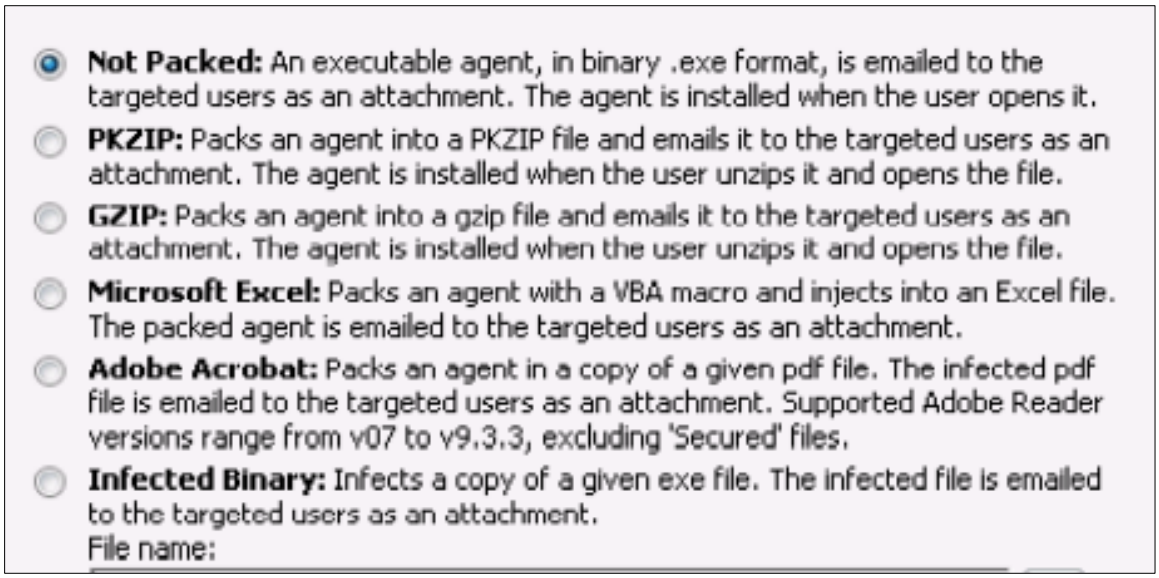

Figure 2 Payload Packaging Options – Illustrates common methods for wrapping malware payloads, including compression formats and embedding within popular document types to evade detection

2.4. Phishing Campaigns and Social Engineering

Phishing is a very popular form of attack because it tricks people instead of targeting technologies. Using accurate domain names and SSL certificates are key in making a phishing attempt seem truthful and safe for victims. Registering domains that sound similar to real ones or using subdomains that are similar to trusted websites, makes it more possible for attackers to interact with victims. By adding wildcard SSL certificates through services such as Cloudflare, communication is safely encrypted, safeguarding websites and making it harder for scams to succeed.

Having a phishing dashboards makes managing and watching the progress of phishing activities much easier. You can view running details on the emails sent and track metrics such as clicks on links and threads taken from compromised accounts. With data, attackers can adjust their activities daily to get maximum results from their efforts. With dashboards, officers can easily sort and filter information from victims, which helps them remain persistent in chasing down clues and leads.

Using different email templates for providers such as Gmail or Yahoo makes the emails look more real. Attackers fashion their emails after official emails, using the right logos, proper format, and correct language. Usually, the attackers send out huge volumes of mails by taking control of or exploiting SMTP servers from online businesses.

Its danger lies in the possibility that, along with credential theft, it can lead to deeper penetration in the network through lateral movement and setting up malware. According to research, being aware of social engineering and trained for defensive actions helps to defend against these dangers (Gomes, Reis, & Alturas, 2020). In addition, in-depth reviews reveal that phishing is flexible and continues to threaten organizations, supporting the need to have several layers of security.

All in all, phishing attacks that are implemented well and make use of domain name systems, SSL certificates, and modern technology can greatly challenge cybersecurity. Red teams should replicate these actions to know how prepared the organization really is.

2.5. Campaign Metrics and Effectiveness

To determine the effectiveness of red team phishing and social engineering operations, the campaign's metrics must be regularly watched and reviewed. Looking at metrics such as the number of targets, email opens, clicks on links, and rates of compliance helps show how users have responded to the campaign. Being able to track activities accurately helps red teams check their progress, develop better ideas, and show the results of their work.

Here, you can see a screenshot of a campaign summary dashboard that captures key information: Includes all targets, the count of people who clicked on damaging links, the number that opened the links without clicking, and the number

that did not. Of the two people in the example, only one of them clicked the link, so the overall compliance rate was at 50%. These dashboards quickly give red teams an idea of how far the campaign has spread, allowing them to find those who are most likely to fall for the attack and plan their continued actions accordingly.

In addition to counting, these dashboards often include charts and diagrams to show how users are interacting with the website. Quick interpretation and decision-making are possible thanks to the visual data collected throughout the engagement. Furthermore, having knowledge of employees who repeatedly default could lead to offering extra training in security awareness to those who need it.

On advanced platforms, you can quickly check and analyze statistics related to clicks, i.e., their times, the addresses of the computers making the clicks, their internet IDs, and the kinds of devices used. With this high level of detail, experts can compare technical evidence with how employees use the system and gain a full picture of the current security state.

All in all, using detailed campaign metrics and reports helps confirm the usefulness of phishing simulations and leads to ongoing improvements in how employees are taught about security. This way, they help protect an organization from various social engineering risks.

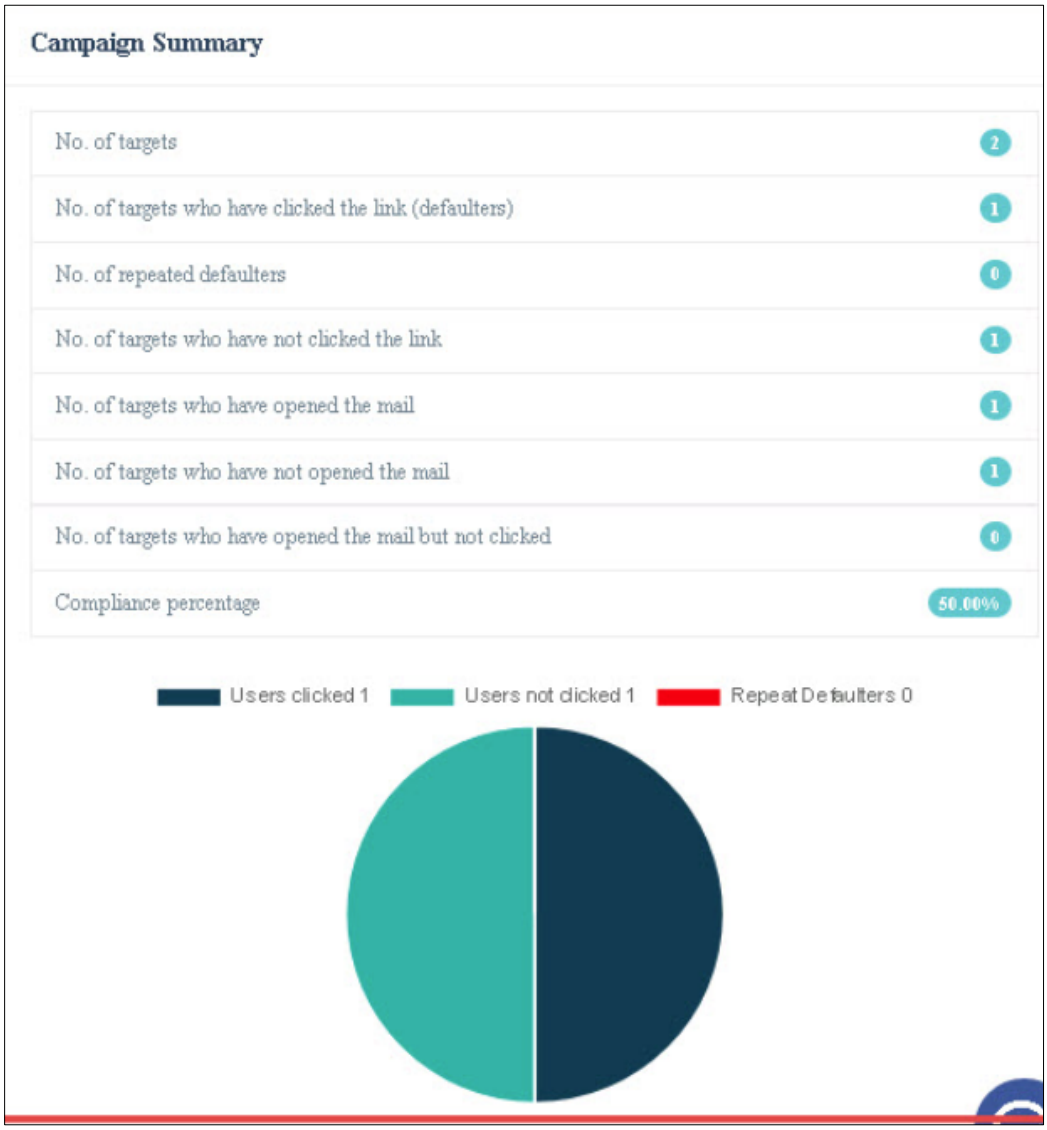

Figure 3 Phishing Campaign Summary Dashboard – Displays key metrics such as targets reached, link clicks, and compliance rates, providing real-time insight into campaign success and user engagement."

2.6. Types of Cloud Attacks and Major Leakages

With more companies using cloud services, the area attackers can exploit has gotten larger, making it easier for them to use mistaken settings and exposed passwords. Very often, cloud attackers start by listing and learning about assets, services, and who can use them on the cloud. Looking for these weak areas allows criminals to take advantage for purposes of gaining higher privileges or stealing data.

Tools like Pacu, Prowler, and Gitrob are now part of regular red team activities. Using Pacu makes it possible to find AWS configurations with security issues and paths an attacker could use to gain access, such as finding unnecessarily permissive roles or buckets that are exposed. By using Prowler, red teams are able to identify security weak points and non-compliance issues inside AWS rapidly. Gitrob confirms if any API keys, account passwords, or tokens have been uploaded to repositories on GitHub by mistake, which attackers might use to take over cloud accounts.

Often, privilege escalation in the cloud targets issues like giving too many permissions or incorrectly setting IAM policies. An attacker who steals a low-privilege account might then use these security flaws to get more access and control over cloud services. As a result, someone may gain access to your data, alter your system resources, or add malicious software.

Even today, key leakage matters a lot because sensitive access keys can be mistakenly stored in public places or given out insecurely. Red teams act out such situations to show the impact of leaked keys in the cloud. Red teams find out about these leaks and use this knowledge to help organizations protect their cloud systems.

Overall, understanding the different ways attacks happen in the cloud and having the right tools is vitally important for red team operations nowadays. As a result, organizations can better deter and respond to recently emerging threats in the cloud world.

2.7. 2FA Bypass and Defense Evasion Techniques

2FA provides additional security on top of the original password-based setup. Yet, advanced cyber criminals and assessment teams have developed multiple tricks to get past 2FA and take over accounts. Taking advantage of bypasses is important for red teams when testing how prepared an organization is in the face of cyber threats.

Some of the most used tools for defeating 2FA are phishing tools such as Evilginx2, Modlishka, and Social-Engineer Toolkit (SET). Using these tools, an attacker can steal login details as they are being sent by injecting themselves in the communication between a victim and the server. Proxying real login processes allows these frameworks to go past 2FA checks, showing that login authentication can be easily bypassed.

Once they have access, attackers try to increase their level of permission in the compromised area. Attackers may compromise limited user accounts and then use vulnerabilities to become administrators and stay for longer in the system. To carry out such attacks, people rely mainly on Mimikatz, SharpSploit, and Empire tools.

It is important for attackers to avoid being noticed by the security team during the evasion phase. It includes things such as injecting processes, camouflaging the source code, and turning off security measures. They use the same malicious actions to see if present security technologies are effective.

In order to do a complete red team assessment, it is necessary to know and practice 2FA bypass and defense evasion techniques. With the use of these simulations, weaknesses in authentication procedures and detection can be found, and organizations can act on these discoveries to build better security and prevent advanced persistent threats.

2.8. Credential Leak Resources and Databases

For red team operations, it is necessary to make use of public databases of data breaches for effective credential hunting and social engineering attempts. As a result, millions of email addresses, usernames, and passwords end up on these sites, helping both cyber criminals and security experts quickly spot correct passwords. Using them allows for better simulation by creating more realistic password spraying and phishing attempts. Here is a summary of important breach sites and data repositories that are frequently used in offensive security work, including their size, how easy they are to access, and their special abilities.

Table 1 Summary of important breach sites and data repositories

Data Breach Search Engine	Description	Actions
DeHashed	Largest & fastest data breach search engine.	Provides a comprehensive database of over 10 billion compromised accounts, usernames, and passwords, allows users to search and monitor email addresses, usernames, and IP addresses.
LeakCheck	Data breach search engine, low price starting from $10/mo, one email address for free, unlimited API, 7B+ entries	Provides users with access to a database of over 7 billion compromised accounts, offers a free trial for one email address, unlimited API access, and affordable monthly pricing.
Have I Been Pwned?	Check if your account has been compromised in a data breach.	Allows users to search their email addresses or usernames to see if they have been involved in any data breaches.
Snusbase	Industry-leading database lookup.	Provides access to a comprehensive database of over 14 billion records, including email addresses, usernames, and passwords, and allows users to search by multiple criteria.
LeakBase	Check if your account credentials have been leaked.	Allows users to search their email addresses or usernames to see if their credentials have been involved in any data breaches.
GhostProject.fr	Industry-leading data breach search engine with over 15 billion records and 7,200 data breaches.	Provides users with access to over 15 billion records and 7,200 data breaches, allowing them to search for email addresses, usernames, and passwords.
Spybot Identity Monitor	Get an overview of where your account was leaked.	Monitors user accounts and provides information on where their information has been compromised.
NuclearLeaks	The biggest free-to-download collection of publicly available website databases for security researchers and journalists.	Provides free access to a comprehensive database of publicly available website databases that have been compromised, allowing for research and analysis.
IntelX	Intelligence X is a search engine and data archive that allows searching Tor, I2P, data leaks, and the public web by email, domain, IP, CIDR, Bitcoin address, and more.	Provides access to a comprehensive database of over 20 billion records, including email addresses, usernames, and passwords, and allows for complex searches using various parameters.
Private Databases	Databases bought in darknet.	Private databases bought and sold on the darknet.

3. Methodology

3.1. Research Design

The approach is similar to other cybersecurity studies that use qualitative methodology to analyze different tools and examine important case studies related to red team activities. Using a qualitative approach, you can get a full understanding of how efforts are made to hack computers in an ethical way. Through careful study of how people perform security tests, use malicious software, and try to trick others, the study helps show just how complicated and tricky these kinds of tests really are. Reviewing cases allows professionals to practice what they learn and find examples of applying different concepts in the real world. It makes it easier for the researchers to observe and understand what methods and strategies the red team is currently using. To paint a clear picture of offensive security, the study highlights the context rather than presenting numbers. With this approach, it is easier to study the progress of cyber risks and how red teams find new ways to test an organization's security measures.

3.2. Data Collection

To gather the necessary data, this study transfers facts from public cybersecurity applications, APIs, and databases of online breaches. Open source tools give a lot of helpful knowledge for looking into how red teams work, because they are regularly used for tasks like checking networks, finding weaknesses, using attacks, and cleaning up after things are done. This information is incredibly valuable for grasping how credentials are used in cyber attacks. This information is also useful, as it allows researchers to see real examples of leakage in databases and study the most common ways data is accessed and used. By using these different sources, data collection helps us really understand what threats and techniques we might be facing from teams trying to hack into systems. Since the approach isn't focused on a specific topic, it better reflects how offensive security tools would be used in practice.

3.3. Case Studies/Examples

3.3.1. Case Study 1: Phishing Campaign Targeting Financial Institution

Adversaries use phishing often, and it's especially successful when targeting the financial sector due to the high value of the data involved. This case study describes a phishing attack that occurred against a mid-sized financial organization and what red team members achieved by carrying out the attack.

Before proceeding, the campaign's team took time to investigate the employees, the company structure, and the main ways they communicate. They gathered a list of valuable targets by collecting information on executives, IT staff, and workers from the finance team using Open Source Intelligence (OSINT) and programs that scan social media. People's names and email addresses were stolen for use in phishing campaigns, making them more successful.

These phishing attempts resembled official emails sent by Nissan employees. The institution's images, styles, and terms were present in every email. They used time-sensitive topics, such as "please reset your password" or "there are changes to your important account," to prevent people from suspecting anything. The emails included links to clever fake websites that looked a lot like the real ones, and the domain parts of these sites were very close to the real institution's domain, so they didn't give off browser warnings and made people trust the sites more.

When hitting the link, they were directed to carefully-made webpages urging them to enter their login information. These pages were made to look and work normally so that they could slip past simple security checks and grab your login details without you noticing. They made great efforts to evade security tools by hiding their activity through user-agent checks and IP filtering. Successful credential capture meant the attackers could get inside the company's network using real user accounts, which helped them get past the company's main security systems.

The red team began moving from one piece of hardware to another within the network once the access had been granted. Accessing Mimikatz, they found ways to discover new credentials and move deeper into the system to locate the sensitive areas. Through legal solutions, they guided themselves in the environment, managing to conceal most suspicious signs and avoid detection at the endpoint. Accessing the internal network from other systems made it possible to use key financial databases and Servers used for email.

Data taken off the network was stolen in a way that wouldn't trigger any alarms. They used encrypted technology to communicate and copied regular data to conceal their messages to other computers. If this data became accessible or if someone managed to manipulate it, it might cause substantial damage to customers.

Recording and tracking the simulated attack during the campaign helped the organization assess their security. The investigation revealed that the company's users, email filters, and network areas could be stronger. Recommendations included making people better at spotting phishing emails, also needing stronger email filters, and making sure only trained people can get into important company systems.

In conclusion, this phishing campaign case study shows why it's important to do full red team exercises that use the types of tricks real attackers would use. By using custom social engineering tricks, trustworthy ways to deliver attacks, and hidden actions after breaking in, red teams can find important security weaknesses and help organizations get better at protecting themselves from harder and more advanced attacks.

3.3.2. Case Study 2: Cloud Compromise via Leaked AWS Keys

Organizations today depend on clouds for their easy-to-use and flexible functionalities. Still, their nature and design can make them unsafe to use and therefore tempting to hackers. This case study looks at what happened when someone

found and used leaked Amazon Web Services (AWS) access keys to get into an organization's cloud systems, showing how big the risk was and how important it is to keep your credential safe and use good cloud security.

AWS access keys were found in a public Git repository, which initiated the attack. These keys, which let people get to the company's cloud, were left at risk because not enough code was checked and the security rules weren't strong enough. Attackers often check public repositories with tools like Gitrob and Shhgit to find any leaked usernames and passwords, so they can use these to break into cloud systems without having to fight through security systems.

As soon as they got the access keys, the attackers started using the API to check the available resources. They discovered several vital resources, for example, data buckets with personal data, machines carrying key operations, and IAM roles with too many permissions. Since the IAM policies were not stringent enough, attackers could take control of important services in the environment.

The attackers were able to launch malicious applications onto the infected EC2 instances. These tasks were designed to set up reliable channels for leadership, scan the system, and help access other areas of the cloud server. Because of this, they could still access the system after the original compromised keys were removed.

Any sensitive data saved in S3 buckets was secretly shared through encrypted paths to avoid detection by anyone monitoring. No one is officially liable for the PII theft and its related privacy and regulatory dangers. The attack also used cloud settings to turn off logging and security alerts, making it much harder to find and react quickly to the problem.

The study showed that the company had not followed strict cloud security rules, such as failing to secure its identity access management system, lacked automation of finding leaked details, and had poor oversight in the cloud. It was suggested to strengthen the security of credentials, follow the principle of least privilege in IAM, and continuously monitor with features for spotting unusual events.

This case shows how important it is to keep cloud environments safe by preventing things like leaked passwords and incorrectly set-up settings. It identifies that threat actors rely on tools and APIs designed for the cloud to establish greater power and stay hidden. Testing the organizations' security with such scenarios helps them learn about their risks and prevent future issues.

3.4. Evaluation Metrics

Red team operation effectiveness should be determined by looking at metrics that show their success in technology and in influencing the organization. The most significant measures are how well threats are being prevented, spotted, and used against a system. The compliance rate shows how many people out of a group actually click on tricks like phishing emails, helping us see how aware people are and how well they picked up the training. Detection avoidance checks how well the red team can stay hidden by getting around tools like antivirus, system watches for break-ins, and security monitoring. A low rate of detection avoidance is a sign that a company's defense and surveillance systems are inadequate. It looks at whether or not the found vulnerabilities were effectively used to access the target, gain more rights, and accomplish the goals. Combining these metrics helps a company better understand how well it stands up to real-life risks, shows which parts are strong and where there are things to work on. These standards help organizations check how their security is doing as time goes on, so they can figure out where to focus their efforts to make things safer, and they are important parts of proper red team assessments.

4. Operations

4.1. Reconnaissance and Scanning

To obtain detailed information, the red team starts with reconnaissance and scanning the target environment. During reconnaissance, red teams gather information about a network's design, what services it has, and the possible ways to get in by looking at open sources and carefully watching the network without actually interacting with it. During this phase, bad actors determine the targets they should focus on. Scanning tools like masscan and rustscan are then used for active network scanning to help find which ports are open and what services or programs might be running, and also to look for any possible security weaknesses. The right reconnaissance and scans allow you to prepare the best assault strategy and limit errors. These activities lay the groundwork for more in-depth security checks and possible cyber-attacks by looking over all the target's digital information and activity. Overall, it is important to perform proper reconnaissance and scan targets to help design the best possible attacks for maximum success.

4.2. Vulnerability Assessment and Exploitation

After scouting out the target, this process looks for and takes advantage of its vulnerabilities. These security tools automatically and manually find outdated software, vulnerabilities in applications, and misconfigurations. It helps red teams identify flaws in the system that may be exploited by an attack. Through Metasploit or Cobalt Strike, criminals can target known weaknesses in a system and attempt to either get access for the first time or gain greater privileges. At this point, the tester checks the efficiency of protection measures and provides helpful information about risks. After exploitation, details of the vulnerabilities are revealed, and red teams become ready to advance further within the system. Carrying out tests diligently results in a realistic software model without interrupting the company.

4.3. Post-Exploitation and Lateral Movement

At this phase, red teams secure their position in the affected system and try to increase their control. Activities include finding ways to get more privileges, stealing things like passwords with tools like Mimikatz, and making sure the attacker can get back in at a later time. Attackers can switch to other parts of the network using lateral movement after gaining control over one host. Movement on the network is made easier with the help of pass-the-hash, remote server attacks, and taking advantage of trusted relationships. Red teams pretend to be opponents by making use of the same tools and rules that original adversaries would use to be undetected. At this step, it is critical to outline how a data breach might impact the company, such as by exposing its confidential information and important systems. It shows where network splitting, access rules, and watching systems might be weak, so organizations get clear ideas on what to do to get better protection inside their networks.

4.4. Clean-up and Reporting

Clean-up and reporting are the last crucial steps in any red team operation. When the engagement is over, red teams take steps to dismantle and remove all the tools, files, and access paths used during the simulation. As a result, this cleanup handles errors before they arise, deletes unneeded flaws, and protects the system's stability. Such an audit helps the organization deal with any issues that might arise once the assessment is done.

All information from each stage of an operation goes into the report, so stakeholders can clearly see what vulnerabilities were found, which they were exploited, and the remaining security flaws. A clear description of how the attacks occurred, the impacts they had, and what actions to take for remediation is found in effective reports. Visual tools such as graphs and dashboards help make difficult technical data understandable for all audiences.

Easily understandable and practical reports allow companies to improve their defenses, plan better for incidents, and make key decisions on security. Additionally, it provides the base for further evaluations, which helps to boost security all the time. Therefore, clean-up operations and reporting close the circle for red teams by adding value and ensuring secure actions.

5. Attack Vector Categories

5.1. Network and Infrastructure Attacks

In such attacks, the primary components used in a business's IT system are targeted. In most cases, scanning and reconnaissance are used at the start to look for open ports, different services, and unprotected devices. Attackers may get access to a network by exploiting unsecure protocols, devices with errors, or firmware that is no longer supported. Examples of techniques include Man-in-the-Middle attacks, polluting DNS information, and taking advantage of weaknesses in routing protocols. Red team attacks allow for evaluation of the effectiveness of separating networks, firewalls, and intrusion detection systems. By successfully attacking infrastructure components, a hacker can cut off messaging, read private files, or move deeper into the network. Understanding the different attack vectors helps companies decide which devices require stronger security and add several layers to their defense. Testing infrastructure security on a regular basis with red teams helps find weak points that other types of assessments may miss. This way of working makes it more difficult for well-equipped adversaries to penetrate the key areas of a company.

5.2. Malware and Payload Attacks

To carry out these attacks, hackers use malware and payloads to sneak unauthorized code into target computers to gain access, stay in the system, or remove important data. Delivery of malicious payloads takes place using executables, macros in Office documents, PDFs, and compressed archives. Using tools like Metasploit, Cobalt Strike, and Empire, red teams are able to produce malware that is hidden and hard to find. Once these malicious files run, they create communication links, so that a hacker can control the system and take data from it. Red teams send simulated malware

to endpoints and observe how well the system and staff identify and stop the infection. Encryption and staged system delivery are used in advanced payloads, which gives them a similar appearance to other typical traffic. Carrying out a malware attack vector review can help organizations improve their antivirus systems, detection tools for devices, and user training. This process closes any openings that malicious actors use to bypass security undetected and stay on the network for a long time.

5.3. Phishing and Social Engineering

It is often through phishing and social engineering that attackers first gain access to target organizations. Such attacks take advantage of how people think, making them fall for lies and carry out damaging actions. Majority of phishing activities use fake websites, well-crafted emails, and modes of interaction that look legitimate. They play out such attacks to assess if people notice suspicious emails and whether email security can catch them. In addition to emails, social engineering can use phone calls, instant messaging, and face-to-face tactics to target employees at any level. The main aim is to judge whether an organization can be affected by manipulation and information leakage. Being aware of risks related to human factors encourages organizations to come up with better learning programs and to introduce controls such as filtering emails, scanning web links, and requiring several authentication steps. By doing this, companies are less likely to fall for phishing and have better protection from developing social engineering strategies.

5.4. Cloud and API Attacks

Such attacks take advantage of weaknesses in both cloud and API systems, as these are now crucial elements in IT infrastructure. Issues such as failing to secure cloud services or exposing buckets of data can allow attackers to enter systems and increase their level of access. Some APIs found in cloud services are vulnerable because they can offer simple authentication or too much access to users. Experts in red teaming use various tools to count up cloud assets, look for secret information, and try to raise their privileges. Doing security simulations with only cloud assets exposed highlights problems with identity, privacy, and remote observation. With more organizations turning to the cloud, it is important to design secure APIs and make sure cloud configurations are robust. Exercises aimed at cloud and API vectors help companies handle issues exclusively found in these systems and avoid any negative effects on their important data or systems.

5.5. Defense Evasion and Persistence

Evading detection by law enforcement and remaining persistent are vital parts of red team attacks. Often, evasion includes hiding the payload, encrypting the code, switching off security tools, and mixing with regular computer actions. Persistence is achieved by installing tasks that run regularly, autostart entries, or setting backdoors to stay in control even when changes are made to the system or credentials. They make use of Mimikatz and Empire to invisible gather user account credentials and climb higher in hierarchy. They focus on seeing how well the organization's system can detect, log, and respond to such attacks. When evasion and tenacity are used successfully, it shows how hard it can be for defenders to catch advanced enemies. This way, red teams provide useful info on how security rules and processes react to different situations. It is very important to enhance evasion and persistence defenses to keep the lasting effect of an attack short and minimize what is lost.

6. Conclusion

6.1. Summary of Key Points

This survey has discussed the full range of Red Team work, mentioning regular attack paths and the defined process used in ethical offensive security testing. To find weaknesses in the systems, red teams carry out initial checks, examines them for vulnerabilities, try to break into them, and examine their remaining activities. Phishing campaigns, malware distributors, cloud attacks, and tactics that target humans, known as social engineering, have been looked into to see their contribution to breaking into systems and networks. The panel stressed that compliance rates, chances of not being detected, and how much damage was done should be used to judge the strength of a red team. In addition, the entire process from lateral movement to cleaning up the system was discussed, to present how engagements progress. Taking this holistic view allows businesses to notice unexpected threats, gain better security, and respond more effectively in emergencies. In essence, the study proves the key importance of red teaming to help organizations prepare for new cyber-attacks during practical simulations.

6.2. Future Directions

Because cyber threats get more advanced and sophisticated all the time, red teams must always be ready to handle them. Moving forward, attention will be given to using cloud-native environments, managing containers with

Kubernetes-like platforms, and securing the rising use of APIs. AI and machine learning give rise to new sensors and tools that can be used either for defense or attack, so red teams should learn how to use these systems. At the same time, attackers are finding new ways to get around multi-factor authentication and avoid detection, so red teams have to keep improving their ways of hiding and staying persistent. Using constant updates of threat intelligence and automation techniques will make simulations more effective and timely. These trends help red teams be proactive, offering a company valuable data and readiness for upcoming attacks. Red team organizations must keep investing in research and new ideas to stay up to date and useful.

References

[1] AL-Otaibi, A. F., & Alsuwat, E. S. (2020). A study on social engineering attacks: Phishing attack. International Journal of Recent Advances in Multidisciplinary Research, 7(11), 6374–6380.

[2] Aibekova and V. Selvarajah, "Offensive Security: Study on Penetration Testing Attacks, Methods, and their Types," 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 2022, pp. 1-9, doi: 10.1109/ICDCECE53908.2022.9792772.

[3] Cuzme-Rodríguez, F., León-Gudiño, M., Suárez-Zambrano, L., & Domínguez-Limaico, M. (2018). Offensive Security: Ethical Hacking Methodology on the Web. Advances in Intelligent Systems and Computing, 127–140. https://doi.org/10.1007/978-3-030-02828-2_10

[4] Elgh, J. (2022). Comparison of adversary emulation tools for reproducing behavior in cyber attacks. DIVA. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1632554&dswid=-5433

[5] H. Holm, "Lore a Red Team Emulation Tool," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 2, pp. 1596-1608, 1 March-April 2023, doi: 10.1109/TDSC.2022.3160792.

[6] Perez, E., Huang, S., Song, F., Cai, T., Ring, R., Aslanides, J., Glaese, A., McAleese, N., & Irving, G. (2022). Red Teaming Language Models with Language Models. ArXiv:2202.03286 [Cs]. https://arxiv.org/abs/2202.03286

[7] Silviu Constantinianu. (2020). Red Team – Critical Thinking Main Tool in the Operations Planning Process –. Romanian Military Thinking, 1, 140–153. https://www.ceeol.com/search/article-detail?id=918692

[8] V. Gomes, J. Reis and B. Alturas, "Social Engineering and the Dangers of Phishing," 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Seville, Spain, 2020, pp. 1-7, doi: 10.23919/CISTI49556.2020.9140445.