Purple teaming in system hacking

University of Turku
Department of Computing
Bachelor's thesis
Computer science
January 2025
Eetu Karhunen

UNIVERSITY OF TURKU
Department of Computing

Eetu Karhunen: Purple teaming in system hacking

Bachelor's thesis, 26 p.
Computer science
January 2025

The cybersecurity world is in a continuous battle with hostile adversaries. In order to keep computer systems safe from breaches, the approaches of cybersecurity professionals need to evolve faster than the adversaries who are trying to find vulnerabilities inside the systems in order to steal data.
The problem that the field of cybersecurity faces in a system hacking concept is that the traditional approaches that have been implemented into the industry might not be the most efficient ones. The traditional red and blue teaming doesn't use communication in the most efficient way. Finding the best approach to defending an organization's assets is crucial.
This thesis explores what is ethical hacking and how it has been imported into organizations cybersecurity training by using red and blue team simulations. Lastly, this thesis compares red and blue teaming against purple teaming. Purple teaming is a new approach to improving system security that can be an upgrade to defending against hostile adversaries. Purple teaming introduces enhanced communication to the red and blue team simulations and it can be implemented into organizations that don't have enough capital for red and blue teaming.

Keywords: Ethical Hacking, Cybersecurity, System Hacking, Cyber Kill Chain, Operating Systems, Red team, Blue team, Purple team

Contents

1 Introduction

The revolution and widespread use of information technology have brought benefits to people, but as the number of different kinds of electronic devices increases, so does the value of stealing data. Most computer networks have been successfully penetrated and this includes critical infrastructures varying from banks to hospitals. As hostile adversaries are trying to improve their techniques in order to improve on stealing data, we must also find new ways of improving the security of the systems that we have. [1] [2]

The cybersecurity world has traditionally used simulations where two teams are divided into attacking and defending. This approach simulates real-world situations where a hostile adversary is trying to get into a system that an organization has in order to do the organization harm for its own benefit. Despite that, we already have an approach that improves the security of organizations. We need to continually enhance the traditional approaches so that organizations can keep up with the ever-growing threat landscape and do not fall behind the adversaries who continuously look for innovative ways to compromise critical infrastructure. In the last ten years, there have been new strategies and approaches devised to improve the communication of the opposite simulation teams in order for them to have better results in improving security. [3] [4]

The motivation for this thesis is to explore and understand the new approaches, whether they provide better results or are just ideas with no concrete improvements.

Our defence must be better than the adversaries, and new approaches to improve overall security are critical to get a head start in the battle against the adversaries. The field of ethical hacking is very broad and comprises different domains such as network security, wireless security, cloud security, etc. In this thesis, we focus on system hacking, which is the act of compromising an operating system by using different hacking software in order to breach the target system and get administrative privileges inside.

This thesis aims to answer the following research questions:

- **RQ1**: What is the traditional approach to system hacking?
- **RQ2**: What is purple teaming in system hacking?
- **RQ3**: What is the difference in the effectiveness of purple teaming compared to red and blue teaming in system hacking, and what is the future of the field?

The sources of the thesis were gathered from different digital databases, including IEEE Xplore, ACM Digital Library, SpringerLink, Web of Science and Google Scholar. In the second chapter, keywords that were used to search digital databases were "ethical hack*" OR "penetration test*", ("ethical hack*" OR "penetration test*") AND ("blue team*" OR "red team*) and ("blue team" OR red team"). For the definition of computer systems there was individual searches made with keywords like "computer system". Most of best sources were found from the IEEE Xplore.

The sources of the third chapter and fourth chapters were found with the usage of keywords like "purple team*" ("purple team*" AND "hack*") and ("purple" AND "hack*"). Finding sources for purple teaming was challenging because many of the latest pieces of work were behind a paywall as the sources were books that had been made in the latest years for training purposes.

The rest of the thesis is organized as follows: The second chapter explains the

fundamentals of ethical hacking and answers RQ1. The third chapter explains the definition of purple teaming and answers RQ2. The fourth chapter analyzes the advantages and disadvantages of purple teaming compared to the traditional approach and gives ideas on how system hacking will be done in the future. The fourth chapter answers RQ3. The fifth and final chapter draws the conclusion from the analysis done in the earlier chapter, summarizes the answers to the research questions, and presents potential future research directions.

2 The fundamentals of ethical hacking

2.1 Definition and history of hacking

A hacker is someone who is trying to get unauthorized access to information in a computer system. Ethical hacking or penetration testing is hacking that is done legally and with the intent to improve the target system's security. Ethical hackers, also known as white hat hackers, use the same set of tools and techniques in an attempt to gain access to the target as hostile hackers. [5] [6]

Hackers who use their toolset for stealing information or planting different kinds of malicious software in the target computer system are called black hat hackers. There are also hackers who place themselves between the white hat and black hat activities, known as grey hat hackers. Grey hat hackers hack into computer systems for their own challenge, but grey hats don't help the victim or cause them harm. [5]

The history of hacking starts in the 1960s and 1970s. These hackers were usually students who had exceptional programming skills, and they would make practical jokes to each other to display their knowledge and ability with technology. Hacking into their institution's own systems by cracking passwords was thought of as a challenge, not something to do in order to financially benefit from it. [7]

Information technology has improved significantly since the 1960s. Hacking in

the 2000s became more financially profitable, and information became something that was used to advertise products to consumers. In the beginning of hacking, the ideological side was more important than the economic one, but in the 2000s, this shifted and economic benefit became more important for the hackers [7].

The first three articles found from IEEE digital library with the topic of ethical hacking or penetration testing are from 2001 and 2002 [8] [9] [10]. The first actual academic article about penetration testing was found in the sources of these articles, and it dates back to 1975. The article focuses on operating system penetration testing [11]. Ethical hacking is already almost 50 years old and not a new thing in the information technology world.

2.2 Definition of computer systems and system hacking

A computer system is a device that is built from two main components: hardware and software. Hardware consists of the physical components inside the computer, such as the processor or the graphics card. Software refers to the applications that are running on the hardware, such as the operating system. An operation system is an application responsible for using the hardware in an efficient way and communicating between the hardware and other software. [12]

System hacking is the act of using hacking software and frameworks to gain unauthorized access to the targeted system with the intention of retrieving sensitive information. [13]

2.3 Red and blue teaming

Red and blue teaming is a concept that dates back to the army and World War I. There are two teams: an attacking and a defending one. The red team is the side which is trying to attack and penetrate the target to get unauthorized access. The blue team is the defending side, which is trying to keep everything safe from the red team. [3]

The red team takes on the identity of actual hostile threats that the organization faces. The red team uses different kinds of tools and techniques in order to breach the organization systems that are typically used by an actual attacker [14]. The red team also has responsibilities such as threat hunting, building custom tools and guaranteeing physical security [15].

The blue team has the responsibility to defend the organization from hostile adversaries, including red team attacks. In the system hacking view, the blue team uses different kinds of monitoring tools to notice the red team's attack as soon as possible. Blue teams have other responsibilities such as: asset protection (laptops, tablets, phones), data protection, network intrusions and detection, identifying and accessing, incident response and vulnerability management. [15]

The red and blue teaming simulation goes in a very straightforward style. Before the simulation starts, the red team needs to get the rules of engagement, where there are different kinds of notes that tell what can be done and what is forbidden [15]. The red team also needs the **Tactics, Techniques and Procedures** (TTPs) that they are meant to simulate and adversary. The TTPs are the actual threats that the organization faces and have been observed in the past from real-world attacks. [16]

When the simulation starts, red team needs to start taking time on two things. Firstly on the Mean Time to Compromise (MTTC) and on Mean Time to Privilege Escalation (MTTP). MTTC starts to run on the clock simultaneously with the actual

simulation. MTTC metric counts the time that the red team takes to penetrate the system successfully. MTTP starts at the same time as the MTTC, but MTTP keeps on running the clock until the target is fully penetrated and the red team has administrative roles inside the target. [3]

The blue team has the responsibility to take time on the Estimated Time to Detection (ETTD) and Estimated Time to Recovery (ETTR). These are the metrics that keep time on how much time the blue team needs to notice that the system is compromised (ETTD) and when the system successfully recovered from the attack (ETTR). [3]

At the end of a simulation, both of the teams share their knowledge on what happened during the simulation and what targets were available and breached [17]. This way, the blue team can make the adjustments to prepare for the next simulation or real attacks. Here is Figure 2.1 that shows a typical red and blue simulation:

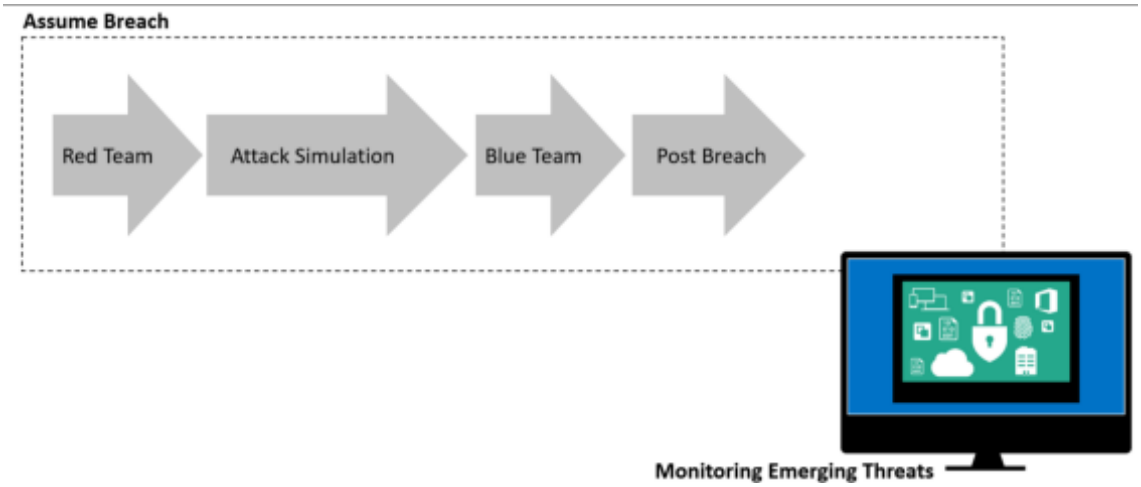

Figure 2.1: An example of red and blue simulation. [3]

In the case that the red team was successful in the attack the blue team starts to save the evidence in order to be able to analyze the data. Validating the evidence in order to be sure about the breach is important, and in the case that a successful attack has been made, the blue team members save the evidence as an Indication of

Compromise (IOC). When the IOC has been captured, the blue team needs to report the details to the people who are relevant to it. Scoping the breach is important when there is enough information gathered on the attack. Lastly, the blue team creates and executes a remediation plan to get the attacker out of the system. [3]

2.4 Methodologies and tools used in system hacking

2.4.1 Red team methodologies

The methodology used in hacking a system includes the following steps: gathering information about the target, scanning, gaining access, maintaining access and clearing tracks [1]. The process of hacking a system does not differ from the methodology followed for ethical hacking. These five stages are also referred to as the **cybersecurity kill chain** [3]. All of these steps are important in order to get into a system but the main process of system hacking starts from the gaining access step and stops at the clearing tracks step. In these stages, hackers use different kinds of hacking tools to break into and control a computer system [13]. We will briefly go into detail in all of these steps including the ones that are not the most essential for system hacking as they are all important for a successful attack.

The first step of hacking a system is gathering information. In this step the hacker collects information close to the target that is publicly available. For example, if the target is a company system, the hacker can gather information about the company's employees who interact with the system. Gathering the employee information includes investigating their social media profiles and, for example, advanced Google searches. These investigations can lead to important information that the hacker can utilize for a successful attack on the target system. The gathering information step also includes scanning the target with different tools to discover the network topology and the devices on the network. [3] [1]

The second step of hacking, gaining access to a system, utilizes the tools and information gathered in the scanning step [3]. Most of the time this phase focuses on cracking passwords with bypassing or cracking techniques. [6]

After gaining access by using different hacking tools, it's time to maintain access so that the attacker can stay in the system undetected and return anytime. Privilege escalation is a method to gain higher privileges (e.g. admin access) that allow the hacker to have better control of the target system. Privilege escalation inside the target system has two categories: vertical and horizontal. Vertical privilege escalation uses tools to achieve its objective of changing to an account with a higher level of authority. In horizontal privilege escalation, the hacker uses the hacked account to elevate it to compromise other accounts for a higher level of authority, but this approach does not include changing accounts. [3]

As the last step of hacking a system, the hacker covers tracks that might have come with the successful attack. This way the hacker stays undetected and is able to do the attack without being caught. Covering tracks means overwriting different kinds of system logs that might have been affected in a way that can expose the presence of the attacker. [13]

Hacking a target is divided into three categories, depending on the amount of knowledge that the attackers have of the target system. These categories are black box, grey box and white box. The term black box means that the red team, or who is trying to successfully penetrate a system, does not have any information about the target. A grey box means that the attacker has some information about the target, for example, an IP address to use in the attack. In the white box approach, the attacker has all the information needed to access the target system or network, source code or the defending tools used for securing the network. In this thesis, we will be focusing on the grey box approach, where the first steps of gathering information are not needed, but other tools like network mapping are required. [18]

2.4.2 Red team tools

There are many tools that can help a hacker breach a system. In this thesis, only some of them are introduced. There are also operating systems that are designed for penetration testers and information security professionals, like Kali Linux, which comes with hundreds of different kinds of hacking tools [4].

Gathering information phase tools

Social engineering is a tool used to get information out of people by following them and getting information about their hobbies, their position at the target company and different points of interest. Social engineering is usually done on social media, but it can also be done directly face-to-face or using phishing techniques such as sending emails or SMS. [3]

Phishing is done by sending emails that have the object of getting the receiver to tell information about the target. Phishing also includes the act of sending malware to the employee in the hopes of getting access to the computer or the computer network of the target. [3]

Nmap is a network mapping tool that a hacker can use to identify what is running on the target computer and what operation system it is using. [3] It also tells what ports are open, filtered and closed. Nmap also assists in identifying the firewall configuration of the target system [3].

Wireshark is a network scanning tool that can be used to capture data that is in contact with the target system. Wireshark gives hackers the ability to view what kind of devices are on the target network, and in the case of a poorly encrypted password change, Wireshark can give valuable information to the attacker. [3]

Gaining access phase tools

Metasploit is a hacking framework used by hackers. When Metasploit is used to scan the target, it scans the operation system and finds the vulnerabilities and payloads that can be used on that operation system type. [3] After that, the hacker can find information about the vulnerabilities and hack into the target. The efficiency of Metasploit can be tested, for example, with the Windows 7 operation system. Windows 7 has not been getting security updates in many years, and it has many high-risk vulnerabilities that a hacker can use.

John the Ripper works by guessing the common passwords using dictionaries [3]. Dictionaries are a word list with the most used passwords. For example rockyou.txt is one commonly used dictionary for hackers, it has 14,341,564 unique passwords. **Hydra** is also a password-cracking tool. Hydra can use dictionary and brute-force attacks to crack the password. Hydra is popular in using fast network login hacking. [3] **Cain and Abel** is a tool to crack different kinds of passwords from the Windows operation system. The tool uses many methods, like network packet sniffing, to crack password hashes. [6]

Maintaining Access tools

Metasploit can also be used for maintaining access as it is a hacking framework. **Beast** is a trojan horse that is used to make back doors into the target system. It is known as a remote administration tool (RAT). [6]

Covering tracks tools

Metasploit and **OSForensics** for deleting log files and registry files. [6]

2.4.3 Blue team methodologies and tools

Blue team uses different kinds of network monitoring tools to detect attacks at the Security Operations Center (SOC). These monitoring tools that the blue team uses include Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), Intrusion Detection Prevention Systems (IDP) and possibly other tools like Endpoint Detection and Response tools (EDR). The blue team may also use machine learning tool integrated within the existing security technologies to help detect an attack when looking at the different monitoring logs. [19] [16] [15] [4]

The blue team monitors various activities, such as network monitoring and alerts generated by the SOC, and is responsible for identity and access management (IAM). IAM is a very important part of blue teaming because it ensures that no one has higher privileges on the systems that they actually need, and an old worker will not have access to the systems of the organization. This means that the red team's goal of MTTP will be harder to achieve when privilege escalation is made more difficult by managing employee privileges. [15]

3 Purple teaming

3.1 Definition of purple teaming

The definition of purple teaming doesn't have official records that are identical between different organizations and sources. Some sources say that purple teaming is done in a way that everyone is a member of the defensive side and the attacking side [20]. Other sources say that purple teaming still does have teams with different specialities of attacking and defending.

Purple teaming is a concept made to improve the traditional practices used in ethical hacking. The approach of purple teaming can remove the idea of one team losing and the other winning. This kind of approach ensures that members of both teams can improve and bond together in order to enhance the security of the organization on a higher level. [4] Here is Table 3.1 that shows what kind of variation the different sources have when defining purple teaming:

Table 3.1: Different purple teaming definitions.

Source (Author, Year)	**People with combined red and blue tasks**	**Red and blue teaming still separate**
Jacob G. (2019)		X
Matthew Hickey et al. (2020)	X	
David Routin et al. (2022)		X
Mike Sheward (2020)	X	

The definition of purple teaming can be said to be any improved collaboration between the red and blue teams when compared to the traditional approach of system hacking. Communication between the teams or inside the single team is an important role in purple teaming. Purple teaming can be more focused on the red team or the blue team, but this varies from different kinds of methods. [21]

3.2 Methodologies and tools used in system hacking

The most typical methodology for purple teaming is the **reciprocal awareness** approach. In this purple teaming methodology, both red and blue teams know equally as much of what kind of actions the other team is doing. This kind of purple teaming approach is good for not being competitive as both sides know each other's goals and targets. The reciprocal awareness approach has the challenge of not imitating real-world attacks well. [21]

Unknowing host approach is a methodology that gives the red team more information about the blue team's actions. The information that the blue team gets can be simply a timeline of when the red team attacks are taking place. The red team knows the details of what has been given as information to the blue team, and this way, the red team can make the attacks more realistic. The unknowing host approach has the disadvantage of having the two teams still in a competitive situation. [21]

Unknowing attacker approach is a methodology where the red team doesn't know anything about the blue team's attributes or activities. The red team does not know that the blue team is being given information about the attacking side's actions. This approach of purple teaming gives valuable information about the way of hacking systems to the blue team. This approach can be done in a way that the blue team doesn't act upon the attack but watches it and tries to get more knowledge on how the adversaries attack. The blue team can make some challenges

for the red team, and this way, they can see how the attackers react to defensive actions. This kind of approach is not likely to be used when trying to improve the security of the system because it focuses more on improving the red team. [21]

Red-handed testing approach is a methodology where the attacks are meant to be seen by the blue team. This kind of red teaming can be automated. Usually, the red-handed testing methodology starts with the red team being easy to notice, and when the attack goes on, the red team starts to use their knowledge more. This means that the attack starts to be harder to notice and the blue team can improve on defending. [21]

Catch and release approach is a methodology where the red team gets tested, and the blue team can see how their incident response works. This means that the attacking side is going to get caught by the defending team, and the red team is then trying to keep their foot in the systems that they have breached. This approach is different in a good way because a threat is not over when it has been noticed, and the blue team can focus on improving action on remediation. [21]

The helpful hacker approach is an improved reporting methodology where the red team helps with fixing the vulnerabilities that they have found during the simulation. This means that the red team does not just make a report about the vulnerabilities but the attacking side gives actual solutions on how their job can be made harder. This approach of purple teaming is the easiest to implement in an organization, and it ensures that the blue team can improve defending attacks in the right direction. [21]

Merged team approach is a methodology where red and blue members are combined into one team where they are taught skills and knowledge about both sides. This approach is very cost efficient and always ready to be in action. Most of the time, red teams are hired from a different company to test the security of the organization, and this can lead to a very expensive and time-consuming approach.

In a merged team methodology, organizations don't need to hire external testers. Merge team approach is popular with smaller organizations. [20]

The tools used in purple teaming are not different from the traditional way of approaching system hacking. The attacks are still performed with some kind of version of the cyber security kill chain and the tools used there to perform the attacks into the system and defending works with the different blue team monitoring tools. The difference is in the communication between the teams.

A good example of a purple teaming approach that makes system hacking more efficient is reciprocal awareness, where information is shared between the teams. When the red team is trying to breach the target system they share the data of what blue team tools are giving as information for the defending side. This means that if an intrusion detection system is not warning the blue team about an ongoing attack, the red team can give feedback instantly to the blue team, and the defenders can fix the problem instantly. [21]

3.3 An example of advanced purple teaming in action

This next protocol is an example of reciprocal awareness in purple teaming. The approach has implemented more roles which ensure that the workflow stays organized.

The purple teaming manager is the person responsible for the whole simulation. The Cyber Threat Intelligence (CTI) function that is part of the blue team, assists the red team plan the attack. This blue team function also identifies the threats that the organization faces in order to make red team attacks as close to the actual hostile adversary ones. The red team's task is to plan the attack according to the directions given by the blue team. The blue team manager is responsible for planning

the defence of the organization and improving on failing parts of the defence after simulations. [4]

We have three different sides working together: the purple team manager, red team and the blue team. The process of purple teaming in this case follows the PEIR model which stands for prepare, execute, identify and remediate. [4] Here is Figure 3.1 that shows the PEIR model cycle:

Figure 3.1: The PEIR model cycle of actions. [4]

The **prepare** step of the PEIR model includes running different kinds of tests. These tests include offensive tests, scans and attacks. Preparing starts with all members being at the same place where it's easy to communicate with each other. The blue team then presents the most important threats of the organization and the red team starts planning the attack with the TTPs that the blue team has presented

to them. In the case that the simulation is done with the black box approach the next step can be skipped. The next step after blue teams presentation and the red teams preparation is that these two teams present the action plan to the blue team, which then prepares themselves according to the details that have been given to them by the presentation of the attacking side. [4]

The **execute** step of the PEIR model starts with red team starting the penetration test. After the attack has started, the blue team should be able to detect and handle it according to the type of intrusion. After attacking and defending, the blue team manager will document the discoveries of the attack to the purple team manager. [4]

The **identify** step of the PEIR model starts with all members of the teams together again like in the first preparing step. Team members communicate the challenges and successes of the attack from each team's own individual point of view. The purple team manager documents the discoveries that this discussion has made. Lastly, all members of the simulation identify the biggest risks and prioritize them in a logical order. [4] This is because risks are different and they are not all evenly important to focus on. By prioritizing the most vulnerable risks first the defense is less likely to get successfully penetrated by actual hostile adversaries.

The **remediate** step of the PEIR model includes the blue team improving their security by fixing the vulnerabilities that their defence might have had before. To improve the defence, the blue team uses the documentation and analysis from earlier steps. After the improvements have been done by the blue team, the red team uses the same type of attack that they used in the execute step. Now the blue team gets the information of the improved defense and is able to make more adjustments in order to improve the detection and answering to the attacks. Lastly the purple team manager and blue team manager document the shown vulnerabilities. [4]

4 The difference in effectiveness in system hacking and future

4.1 The difference in effectiveness of the approaches

In the subchapter 4.1.1 we analyze the advantages that purple teaming implements and in what kind of ways purple teaming is better than the traditional approach. In the subchapter 4.1.2 we analyze the advantages of the traditional red and blue teaming and what kind benefits it still has over the new approach.

4.1.1 Purple team advantages

The traditional protocol of red and blue teaming tries to improve security by having the opposite teams have different objectives, limitations and approaches when improving system security. This can lead to flaws in the security of the organization that the teams are trying to improve and protect. [4]

Red and blue teams might be missing new TTPs that have been released, and in purple teaming, the different members can communicate more efficiently in order for this to not happen. The scope of what kind of simulations are going to take place can be different when asking the red team members compared to the blue team's idea. The aligning of views is important for a successful simulation, and this is easier to reach in purple teaming, where communication is key. If red and blue teaming

is done once a year to test organizations defense, it does make it less efficient than purple teaming where purple teams can continuously test the security. [4]

Red and blue teams might not have the needed knowledge about the target system. Purple teaming ensures that both teams get more knowledge and that they can improve their techniques during the simulations. Purple teaming helps the defenders to understand the attacker's methods by being able to communicate about the layers of attack and get data about these phases. [4]

One of the problems that leads to stress in red and blue teaming is that the approach leans towards competition with the other team. The success of the other team leads to the failure of the opposing side. Purple teams work towards one goal, which is system security, where they share their knowledge about possible vulnerabilities in order to make the systems more secure. [4] Blue teams use whitelists for their SIEM and EDR detection. This might be a way in for an advanced attacker, and in purple teaming, the whitelists can be shared, and this way, the blue team can improve on detecting attackers from whitelisted network traffic. [4]

The main point that purple teaming does better is communication and by exposing the attacking side to the blue team's methods and the other way around, it makes the security of organizations better because the attacking side doesn't dive into the easiest detection and the defending side can learn to protect the organization from more evolved attacks. [15]

In conclusion, the advantages of purple teaming are that it can be more cost-efficient than red and blue teaming as it doesn't necessarily need that many staff members, but this might be different from what kind of purple team dynamics the organization has. One of the advantages is that defending systems with an attacker's mindset will promote defence in a way that can be more efficient. Purple teaming has the advantage of being able to improve the safety of the target system while the attack is in action and this leads to a more agile way of improving security. [15]

4.1.2 Red and blue team advantages

The problem with the sources of purple teaming is that they are, most of the time, obviously biased towards purple teaming being the better way of working. As purple teaming is a fairly new concept in the cybersecurity world, there is no actual data from putting purple teaming against red and blue teaming. The red and blue teaming articles do not have sections where they tell why organizations should use red and blue teaming instead of purple teaming. We need to analyse the possible negative sides of purple teaming by looking at what it takes out of the traditional approach.

Purple teaming takes out the competition of enhancing the security of organizations. Competitive scenario better replicates actual real world scenarios where black hat hackers are trying to break into the target systems. In the traditional approach the opposing teams of defending and attacking can actually develop those skills that are needed when an actual attack is happening. The pressured situation makes members of both teams improve their decision-making in quick situations and how to react to different kind of scenarios that they might have not faced before. This is something that purple teaming doesn't always have depending on the methodology that the organization uses. [22]

Another advantage of competition in red and blue team simulations is that it improves the communication inside the teams, and this approach leads to better teamwork in pressured situations [22]. The act of competition helps with simulation members being sharp and eager to get more knowledge in order to win the opposing side [22]. Competition gives the blue team a better mindset when facing the actual adversaries in the actual world by performing pressured situations to the team.

One concern of the new methodology is the fact that the approach of purple teaming, where everyone does attacking and defending, might not be able to give the team members tools to improve and specialize in the best way. By this, I mean

that when an employee is trained to both attack and defend, it prevents the attackers from focusing on just one side, and then attacking can become less skillful and vice versa for defending. This can lead to a less efficient approach than a competitive red and blue team where people are more professional in the opposite actions.

The usage of purple teaming can lead to problems with people. When the teams are giving information to each other, the opposing sides can use this in an improper way. An example would be a blue team that catches everything that the red team does because they, as the defending side, have been given all the details about the attacker's plans and actions. This way of using communication is bad for the security of an organization's systems, and this doesn't simulate a real-world attack. Purple teaming needs to be done with professionals who know how to do it effectively. This can be a problem inside organizations that have used a competitive red and blue teaming before and are still having the mentality of winning against the other team. [21]

4.2 The future of system hacking

The future of system hacking seems to be going towards purple teaming. Purple teaming can be implemented in the organization with many different kinds of methodologies and approaches. Even though purple teaming does have its own challenges, the different approaches of action can be tested, and this way, the best practices for the specific organizations can be implemented. Purple teaming makes red and blue teaming more efficient with the added communication that the traditional methodology has had an insufficiency. Smaller organizations that don't have the finances to do full-scale simulations can implement a merged purple team methodology that is more efficient than just a blue team that doesn't get challenged.

In conclusion, purple teaming will most likely be used as a form of cybersecurity training in the future instead of red and blue teaming, but in many different ways

that the specific organizations have to decide what is best for them. An organization that doesn't use purple teaming at all is not using its resources in the smartest course of action. The helpful hacker methodology is at least something that everyone should be doing when fixing the vulnerabilities after basic red and blue team attack simulations.

5 Conclusions

In this thesis we tried to find answers to research questions about system hacking and the advances that the field has had recently. Finding new approaches that are more efficient than the traditional ones is crucial in the cybersecurity world because hostile adversaries seek to make their own methodologies better in order to breach defenses. This leads to continuous battle between the white hat hackers and the black hat hackers where every way of progression is important.

RQ1: This research question was answered in chapter two. The traditional approach to system hacking is red and blue team simulations. In these simulations, the two teams take on the responsibilities of an attacker and a defender. The red team tries to breach the systems that the blue team protects. During these simulations, the two teams work independently in isolation without communication or feedback. Isolation leads to the opposite teams going to a competitive environment where employees feel stressed and pressured. The competitive environment doesn't favor communication between the teams and because of this vulnerabilities can be fixed with incorrect methodologies that still have the issue.

RQ2: This research question was answered in the third chapter. Purple teaming is an approach where red and blue teams are used in further collaboration than in the traditional approach of system hacking. The benefit of purple teaming comes with the added communication which helps with fixing vulnerabilities sooner and in a way that future breach attempts are successfully defended. The challenge of

defining purple teaming is that the methodologies that are used are different from organization to organization so we have to settle in a broad answer.

RQ3: This research question was answered in the fourth chapter, and the conclusion was that purple teaming enhances the security of the organization's systems by having more communication with the different sides of the simulation, which makes it easier to fix vulnerabilities that have been found. The improved communication between the teams also makes misunderstandings less common. The future of system hacking is going towards purple teaming with its different kinds of methodologies and approaches.

Depending on the situation/scenario, one approach might be better than the other. There are a few things to consider before choosing the right approach which are discussed as follows:

- Constitute the team with the right skill set
- Scope of the project for example, you are interested in finding vulnerabilities
- Criticality of the infrastructure
- Resource constraints

Constituting the team with a right skill set is crucial in order to be successful against hostile adversaries. A purple team that doesn't have proper red team experience will not be able to simulate attacks as well as a traditional red and blue team simulation.

Scope of the project is another important view when thinking about the approach that is the best. When doing a project that has the goal of finding many vulnerabilities, purple teaming in a unknowing host or reciprocal awareness approach is the best. These approaches allow the red team to get every detail about the target and be the most efficient when doing attacks.

Criticality of the infrastructure that the teams are working for is something that needs to be thought of. Purple teaming is good for always being ready for action but if the target is very critical like a banking service, an external red team attack can be beneficial.

Smaller organizations that don't have capital to spare benefit from implementing merged purple team dynamic. External red team attacks can be very expensive and blue teams need to be tested regularly in order to be sure about their efficiency at defending and detecting attacks. A purple team helps smaller organizations to test their defense without heavy financial setbacks.

Future research should be done on how purple teaming and red and blue teaming affect people's mindset when working. At the time of making this thesis, there aren't studies made comparing red and blue teaming and purple teaming with actual numbers on how many vulnerabilities both of them can fix in the same kind of environment. Most of the purple team sources are biased towards purple teaming being the future but there should be actual competitive studies made of how it can actually improve the performance of the cybersecurity professionals.

In conclusion, purple teaming is a new thing that needs more research, but the data that we have at the moment leans towards it being the superior approach as it enhances workflow and decreases stress among cybersecurity professionals in this field. Future research directions could include case study comparisons between the traditional and new approaches.

References

[1] T. Yash, Dinki, S. Kumar, and K. Sharma, "Ethical hacking: A technique to enhance information security", in *2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON)*, IEEE, 2022, pp. 780–784. DOI: 10.1109/COM-IT-CON54601.2022.9850601.

[2] G. S. Rao, P. Kumar, P. Swetha, and G. BhanuKiran, "Security assessment of computer networks -an ethical hacker's perspective", in *International Conference on Computing and Communication Technologies*, IEEE, 2014, pp. 1–5. DOI: 10.1109/iccct2.2014.7066756.

[3] Y. Diogenes and E. Ozkaya, *Cybersecurity - attack and defense strategies: infrastructure security with red team and blue team tactics*, 1st edition. Packt Publishing, 2018.

[4] D. Routin, S. Thoores, and S. Rossier, *Purple team strategies : enhancing global security posture through uniting red and blue teams with adversary emulation*, 1st ed. Packt Publishing, 2022.

[5] G. Vishnuram, K. Tripathi, and A. Kumar Tyagi, "Ethical hacking: Importance, controversies and scope in the future", in *2022 International Conference on Computer Communication and Informatics (ICCCI)*, IEEE, 2022, pp. 01–06. DOI: 10.1109/ICCCI54379.2022.9740860.

[6] S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, "Ethical hacking: The need for cyber security", in *2017 IEEE International Conference on*

Power, Control, Signals and Instrumentation Engineering (ICPCSI), IEEE, 2017, pp. 1602–1606. DOI: 10.1109/ICPCSI.2017.8391982.

[7] M. Christen, B. Gordijn, and M. Loi, *The Ethics of Cybersecurity*. Springer International Publishing, 2020. DOI: 10.1007/978-3-030-29053-5.

[8] B. Smith, W. Yurcik, and D. Doss, "Ethical hacking: The security justification redux", in *IEEE 2002 International Symposium on Technology and Society (ISTAS'02). Social Implications of Information and Communication Technology. Proceedings (Cat. No.02CH37293)*, IEEE, 2002, pp. 374–379. DOI: 10.1109/ISTAS.2002.1013840.

[9] C. C. Palmer, "Ethical hacking", *IBM Systems Journal*, vol. 40, no. 3, pp. 769–780, 2001. DOI: 10.1147/sj.403.0769.

[10] D. Geer and J. Harthorne, "Penetration testing: A duet", in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, IEEE Comput. Soc, 2002, pp. 185–195. DOI: 10.1109/CSAC.2002.1176290.

[11] R. R. Linde, "Operating system penetration", in *Proceedings of the May 19-22, 1975, national computer conference and exposition on - AFIPS '75*, ACM Press, 1975, p. 361. DOI: 10.1145/1499949.1500018.

[12] J. M. Garrido and R. Schlesinger, *Principles of modern operating systems.* Jones and Bartlett, 2008.

[13] C. M. Rakshitha, "Scope and limitations of ethical hacking and information security", in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, IEEE, 2020, pp. 613–618. DOI: 10.1109/ICESC48915.2020.9155846.

[14] C. Chindruş and C.-F. Căruntu, "Enhancing cybersecurity readiness through the red and blue team competition", *Bulletin of the Polytechnic Institute of*

Iași. Electrical Engineering, Power Engineering, Electronics Section, vol. 69, no. 2, pp. 35–56, 2023. DOI: 10.2478/bipie-2023-0008.

[15] M. Sheward, *Security operations in practice*, First edition. BCS, The Chartered Institute for IT, 2020.

[16] B. Kotwani, M. R. Sawant, and D. S. Chopra, "Red teaming vs. blue teaming: A comparative analysis of cybersecurity strategies in the digital battlefield", *International Journal of Scientific Research in Engineering and Management*, vol. 07, no. 12, pp. 1–11, 2023. DOI: 10.55041/ijsrem27675.

[17] C. Chindrus and C. F. Caruntu, "Development and testing of a core system for red and blue scenario in cyber security incidents", in *2022 15th International Conference on Security of Information and Networks (SIN)*, IEEE, 2022, pp. 1–7. DOI: 10.1109/SIN56466.2022.9970546.

[18] A. A. Alghamdi, "Effective penetration testing report writing", in *2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, IEEE, 2021, pp. 1–5. DOI: 10.1109/ICECCME52200.2021.9591097.

[19] O. Akinrolabu, I. Agrafiotis, and A. Erola, "The challenge of detecting sophisticated attacks: Insights from soc analysts", in *13th International Conference on Availability, Reliability and Security (ARES 2018)*, ACM, 2018, pp. 1–9. DOI: https://doi.org/10.1145/3230833.3233280.

[20] M. Hickey and J. Arcuri, *Hands on hacking: Become an expert at next gen penetration testing and purple teaming*. Wiley-Blackwell, 2020. DOI: 10.1002/9781119561507.

[21] J. G. Oakley, "Purple teaming", in *Professional Red Teaming*. Apress, 2019, pp. 105–115. DOI: 10.1007/978-1-4842-4309-1_8.

[22] C. Chindrus and C. F. Caruntu, "Securing the network: A red and blue cybersecurity competition case study", *Information (Basel)*, vol. 14, no. 11, pp. 587–, 2023.