

# ***Penetration Testing (BSHCYB4)***

Student Name: Youssef Alij  
Student Number: X20252561  
Module: Penetration Testing  
Lecturer: Eugene McLaughlin  
Date: 07/04/2025

## Contents

Q1:.....	3
Clearly Defined Objectives .....	3
Rules of Engagement: .....	3
Importance of Scope: .....	5
Data & Communication Handling: .....	5
Conclusion: .....	6
Q2:.....	6
History of Red & Blue in Cyber Security:.....	6
Introduction .....	7
Roles and Functions of Red vs Blue .....	7
Advantages & Disadvantages of Red Team: .....	8
Advantages & Disadvantages of Blue Team: .....	8
Who to Choose Red vs Blue? .....	9
Conclusion .....	10
Q3:.....	10
Introduction:.....	10
Home Security Analysis & Factors Involved: .....	11
Objectives of The Red Team Assessment: .....	11
Steps & Tasks to Test the Home network:.....	12
Conclusion .....	14
Q4:.....	14
OpenVAS Vulnerability Report:.....	14
Description: .....	14
Impact: .....	16
Recommended Remedial Measures:.....	17
References:.....	18

Note: Referencing style in this essay is IEEE (including intext-t citations)

## Q1:

Penetration testing (also known as ethical hacking) involves simulating real-world cyberattacks with the goal of identifying security weaknesses in an organisation's infrastructure, system, applications, or personnel. However, unlike a typical cyber-attack (usually performed by Black / Grey hat hackers) penetration testing is carried out with full authorization of the involved parties, ensuring that there is a clear legal framework, and mutual understanding between the tester and the client. In this case, the "Letter of Engagement (LoE)" becomes indispensable, as it acts as a legal contract and operational blueprint that defines the terms under which the test is conducted.

I fully agree with the states that "A letter of engagement is a vital part of a penetration test". This document is crucial because it ensures that all activities that are conducted by the tester are authorise and are within the testing scope. Furthermore, the documents ensures that expectations are aligned and that risks are mitigated. It establishes accountability, protects both parties from legal reputational harm, and enables the tester to conduct an effective, ethical, and goal-driven assessment.

## Clearly Defined Objectives

As discussed, the Letter of Engagement is a formal agreement between the involved parties that outlines the terms of the engagement. This typically includes the scope, service-level expectations, fees, deliverables, legal conditions, and testing timeline. Every penetration test must begin with a clear articulation of why the test is being conducted, this the first critical section in the letter of engagement (LoE). It outlines the clients' motivations, such as compliance with standards (e.g ISO 27001, PCI DSS), testing incident response capabilities, or assessing new and existing infrastructure for vulnerabilities.

Clearly defined objectives shape the direction and depth of the test, this is important for a penetration tester because it influences the methods and techniques used by the tester. For instance, if the goal is to simulate a real-world black-box attack, the engagement will rely on stealth and the tester's minimal knowledge of the system. Contrarily, if the objective is to verify patch management and secure configuration (software / operating system security patches and best practices), the test may take a white-box testing approach with full access provided to the tester.

Clearly defined objectives is not just helpful for planning, but also crucial for legal reasons. It serves as evidence that all activities and tasks were done within agreed parameters, thereby protecting the tester and consulting company from accusations of misconduct. This alignment ensures that the objectives and test results are tied directly to the clients' specified goals.

## Rules of Engagement:

The Rules of engagement (RoE) and Letter of Engagement (LoE) are interconnected documents that define the scope and boundaries of the testing process. Although these two documents are related, they are distinct concepts in penetration testing.

The rule of engagement is essentially a document that provides detailed guidelines and constraints for the tester, whereas the letter of engagement established the overall contract agreement between the client and the testing firm (or consulting firm).

The Rules of Engagement (RoE) dictates how the penetration test will be conducted. This includes the permitted tools, techniques, and timing of the test. It is designed to reduce the risk of system damage, service disruption, and data loss.

It is crucial to have a well defined “RoE” as it defines the scope, boundaries, and expectations for the penetration tester. It acts as a road map for both the client and testing team, ensuring a controlled and ethical process. As for the tester, it clarifies what is in-scope (what systems or applications are to be tested) and out of scope (what is off limits). Additionally, the ROE also specifies acceptable testing methods, timing and potential consequences of findings. This aspect reflects the ethical obligation under the EC-Council Code of Ethics, which requires testers to “ensure all penetration testing activities are authorized and within legal limits” [1].

Failure to establish a clear a rules of engagement document (RoE) can lead to miscommunication, this may result in outages or data breaches during testing, putting both the client and tester at serious legal risk.

*Example of a Rules of Engagement short template:* (template from <https://csrc.nist.gov/pubs/sp/800/115/final> [2])

- **Objective:** Assess the security of ACME Ltd’s web application and internal network to identify exploitable vulnerabilities.
- **Testing Window:** 15th–22nd April 2025, Monday to Friday, between 18:00 – 02:00 (off-peak hours only).
- **Allowed Techniques:** Network scanning, web application testing (OWASP Top 10), Wi-Fi assessment.
- **Prohibited Techniques:** Denial-of-Service attacks, physical intrusion, testing of third-party or cloud-hosted systems (e.g AWS).
- **In-Scope Assets:** Public web app (myCompany.YJ.com), internal IP range 192.168.10.0/24, VPN gateway, guest Wi-Fi network.
- **Out-of-Scope Assets:** Production databases (192.168.15.0/24), email infrastructure, third-party services (e.g., Salesforce).
- **Data Handling:** All data will be encrypted (SHA-256), handled confidentially, and shared only with the designated security contact.
- **Reporting:** Critical vulnerabilities will be reported immediately to the primary contact for escalation and action.
- **Primary Contact:** Youssef Alij – Security Manager – youssef.ali@agri.gov – +353 86 123 4567.
- **Compliance:** All activities will follow EC-Council’s Code of Ethics, Irish law (Criminal Justice Act 2017), and GDPR regulations.

## Importance of Scope:

Scope defines the boundaries of the engagement in penetration testing, it defines the boundaries and objectives of the testing process. This is arguably one of the most critical sections in a letter of engagement, this is because having a clear scope prevents the test from becoming too broad or too narrow, but mainly it protects critical infrastructure from being accidentally disrupted and helps the testing team focus efforts on approved assets.

It also provides legal protection by ensuring that only authorized systems are tested. This is especially relevant under laws like the Criminal Justice (Offences Relating to Information Systems) Act 2017 (Ireland) and the Computer Misuse Act 1990 (UK) [3][4].

A common and serious issues in when penetration testers inadvertently target third-party services without explicit authorization. For instance, conducting tests and scans against a cloud service provider (e.g AWS) without prior consent could result in several legal consequences, potentially posing both the client and the tester to a lawsuit, contractual breaches, or even in severe cases criminal liability.

The scope is often a formal part of the contract between the customer and the penetration testing service provider. Clearly defining the scope is essential, as it helps prevent misunderstandings, minimises the risk of legal complications, and ensures that the test results are aligned with the organisations security objectives and business priorities. Although, the “Letter of Engagement” and the “Rules of Engagement” together define the scope of the test, it is important to acknowledge that the scope may change during the testing process. This is due to findings or unforeseen circumstances, necessitating flexibility and ongoing communication between all parties involved.

## Data & Communication Handling:

In penetration testing the handling of data and communication is crucial, this is to ensure a successful and ethical process throughout the testing phase. Penetration testing will often uncover highly sensitive data, such as weak passwords, personal information, or vulnerable systems that could be exploited.

Ethical penetration testers must handle sensitive data with care, avoiding misuse or disclosure of this information. Typically, this would be defined in the Letter of Engagement on how the data is to be handled. This includes the collected data (e.g screen captures / logs), stored data (encrypted storage, access-controlled), transmitted (e.g via encryption channels like PGP email), and disposed of (e.g data that is deleted securely after reporting).

Furthermore, establishing a clear communication between the client and other relevant parties is crucial for addressing issue promptly, receiving timely updates, and final reporting and format delivery.

The level of professionalism and the ethical duties that a penetration tester is bound by, ties to how securely and respectfully this data is managed, regardless of the tester’s personal views on

the information uncovered. This obligation is reinforced by the EC-Council's Code of Ethics, which explicitly states that testers must "keep private and confidential information gained in your professional work" [5].

## Conclusion:

In summary, I believe that the letter of engagement is a critical component of any penetration testing engagement. It not only establishes the legal and ethical foundation of the test but also ensures clarity, accountability, and mutual understanding between the tester and the client. By clearly outlining objectives, scope, rule of engagement, and data handling protocols, the Letter of Engagement protects both parties from potential legal and operational risks. It promotes professionalism, aligns the testing process with business needs, and reinforces adherence to industry standards and ethical guidelines, such as those outlined by the EC-Council. In a technical field where even a minor misstep can have serious consequences, a Letter of Engagement is not just important, its essential for conducting responsible and effective penetration testing.

## Q2:

### History of Red & Blue in Cyber Security:

Cybersecurity is a field focused on protecting computer systems, networks, and data from unauthorised access, damage, or theft. It involves implementing processes, controls, and technologies to safeguard against various cyber threats.

In our current time, organisations face constant threats from malicious actors seeking to exploit vulnerabilities in systems, networks and human behaviour. To counter these risks, two distinct approaches have emerged in the cyber security field, "Red Team" and "Blue Team" operations.

A Red Team simulates real-world cyberattacks to identify weaknesses, while the Blue Team focuses on defending systems by detecting the attack, responding to it, and mitigating the threat. For an organisation with limited resources, choosing between the Red team and Blue Team is a critical decision that influences a organisations security priorities, existing infrastructure, and risk profile.

In this essay I will be exploring the roles, advantages, and limitations of both teams, ultimately arguing that, for most organisations constrained to a single team, a Blue Team offers greater value due to its focused on continuous defence and resilience against evolving threats.

## Introduction

Cyber security is a dynamic battlefield where organisations must proactively, on a constant basis protect their assets and learn from potential weaknesses (whether an attacks on the company itself or other companies). Here is where the red and blue team come in, as both teams represent complementary strategies in this effort.

The Red Team adopts an offensive mindset, mimicking adversaries to uncover vulnerabilities through simulated attacks, such as penetration testing and social engineering. On the other hand, a Blue Team takes a defensive stance, where their main objective is to monitor systems, analyse threats, and implementing safeguards with the goal of ensuring operational security. When an organisation is limited to only one team, the choice ultimately depends on whether proactive vulnerability discovery or robust defence is more critical to the organisation's survival. However, to determine this, I will be evaluating both team's contributions, taking into account factors such as cost, impact, and alignment with the organisation's needs, to determine which is the better investment for a resource-constrained entity.

## Roles and Functions of Red vs Blue

To make an informed decision on whether to hire a Blue or Red Team, it's essential to understand what each team does. The Red Team operates as ethical hackers (white hat hackers) employing techniques like network scanning, phishing simulations, and exploit development (code vulnerabilities) to test an organisations' defences. The main goal of the Red Team is to emulate a real-world scenario where a cyber-criminal is attempting to harm the organisation. This can range from script kiddies to advanced persistent threats from skilled cyber criminals, this ensures that the Red Team can expose these weaknesses and vulnerabilities before attackers do.

For example, consider a scenario in which the Red Team successfully exploits a misconfigured server to gain unauthorized access, exposing weaknesses in patch management and firewall configuration. While the Red Team does not remediate these issues directly, their findings are documented and reported, allowing the organization to strengthen its security posture.

According to the **NIST SP 800-115 framework guideline** for security assessment and testing, the Red Team activities align with penetration testing methodologies, focusing on "identifying exploitable vulnerabilities [6, 7] (Scarfone et al. 2008).

In contrast, a Blue Team is the organisations defensive line, responsible for defending the organisations information system and assets against cyber-attacks, with the main focus on maintaining and strengthening its security framework. Their tasks usually include configuring firewalls, monitoring intrusion detection systems (IDS), analysing system logs for suspicious activity, and responding to incidents. The Blue Team also conduct threat hunting (search for threats) to proactively identify risks and implement remediation strategies, this includes implementing security patches and updating access controls. According to the **EC-Council**, the Blue Team is described as the "defenders who ensure systems remain secure against live threats" [8, 9].

To better understand how a blue team would operate in a real-world scenario, image a ransomware attack targeting an organisation. The Blue team would respond by promptly isolating affected systems to contain the threat, initiating the recovery process using secure backups, and conducting a thorough investigation to identify the attack vector and implement measures to prevent further harm [8, 10].

Both the Red and Blue Team are vital for any organisation's security. However, their approaches differ as the Red Team provides snapshots of vulnerabilities through periodic assessment, while the Blue Team offer ongoing protection and incident response. When it comes to an organisation that is only limited to one team, the question is which delivers more immediate and sustained value when resources are scarce.

### Advantages & Disadvantages of Red Team:

If an organisation were to hire a Red Team, one of the most significant advantages would be its ability to uncover hidden weaknesses that might otherwise go unnoticed. By thinking like attackers, they not only identify technical vulnerabilities but also procedural and human related flaws such as employees falling for phishing emails.

Having a successful Red Team engagement can yield actionable insights, allowing organisations to prioritise remediation efforts. One good example is the 2023 Verizon Data Breach Investigation, which reported that 74% of breaches involved human error, underscoring the value of the Red Team exercises like social engineering tests [11].

However, the Red Team also have limitations, especially for organisations with limited budget. Their assessments are typically time bound, providing a point in time view rather than continuous protection that a Blue Team would provide. If the vulnerabilities discovered are not promptly addressed, the Red Team's findings become obsolete. Since the Red Team's primary goal is to identify (not fix) these issues, unremedied flaws may persist, leaving the organisation exposed to new or evolving threats.

Additionally, The Red Team's activities can be expensive, requiring skilled personnel and tools like Metasploit, Open-VAS, and Burp Suite. For a small organisation, the cost of a single Red Team will might consume resources which could be utilised elsewhere for basic defence rather than offense (e.g anti-virus software, employee training, IDS systems). Without a Blue Team in this scenario to implement recommendations and mitigation strategies, Red Team efforts may yield limited long-term benefits.

### Advantages & Disadvantages of Blue Team:

Opposing to how the Red Team operates, the Blue Team offers a proactive and reactive defence, making them the backbone of an organisation's security operations. They monitor systems in real-time, detect anomalies, and respond to incidents, ensuring continuity of business operations. For example, a Blue Team might use a Security Information and Event Management (SIEM) system to identify a brute-force attack and block the attacker's IP address. Their focus on resilience aligns with standards like **ISO 27001**, which emphasizes continuous monitoring and



improvement. Blue Teams also enhance employee awareness through security training and webinars, reducing risks like phishing susceptibility.

However, the primary limitation of the Blue Team is their reactive nature in some context. Without Red Team testing, the Blue Team may lack insight into obscure vulnerabilities, such as zero-day exploits. In terms of costs, the Blue Team would also require investment in various tools (e.g IDS, SIEM, EDR) and skilled staff in order to perform their jobs efficiently.

The investment in the Blue Team for big and small organisations is always a priority, as these costs support ongoing operations rather than one-off engagements. Therefore, having a Blue Team is a priority, as their ability to adapt and respond to live threats makes them versatile in comparison with the Red Team.

### Who to Choose Red vs Blue?

When it comes down to choosing between the Red and Blue Team, this decision ultimately comes down to the organisation's needs and threat landscape. A Red Team is ideal for organisations with robust defences seeking to validate their security posture. However, for most organisations, especially small to medium sized enterprises with limited budget, a Blue Team is a better choice.

This is because threats in cybersecurity is an ever-evolving field, with new threats and vulnerabilities emerging as technology advances. Blue Team offers continuous protection against these dynamic threats by actively monitoring systems, mitigating risks, and responding to incidents in real time. Therefore, they are better equipped to manage immediate and more common risks, such as malware infections, phishing attempts, and insider threats, all of which are far more likely to affect day-to-day operations.

While one could argue that a Red Team would be valuable in detecting sophisticated or advanced attacks, the likelihood of such event affecting a smaller organisation is relatively low. A Red Team might be very well and effective in identifying vulnerabilities, but without resource to remediate them, the exercise is futile. Contrarily, a Blue Team can establish baseline defence firewalls, endpoint protection, and monitoring, while training staff to recognise phishing attempts. Over time, these efforts build resilience in an organisation, thus reducing the likelihood and impact of breaches.

Recent data reinforces this point, as a 2024 study by the Ponemon Institute found that organisations with dedicated incident response teams (Blue Teams), reduces the cost of data breaches by 34% compared to those without [14]. Interestingly, 75% of companies that increased their investment in insider risk management (area handled by Blue Team) did so to improve the return on investment (ROI) of their existing security tools and overall cybersecurity program [15]. As a result of these data breaches, this highlights not just the defensive value of a Blue Team, but also its role in making security spending more effective.

Blue Team also plays a pivotal role in helping organisations meet regulatory requirements such as General Data Protection Laws (GDPR), which mandates continuous security and monitoring, as well as timely incident reporting [16].

For small to medium sized enterprises operating under compliance pressure, a Blue Team ensure not only adherence to legal obligations, but also proactive risk mitigation. While the insights provided by the Red Team are undoubtedly valuable, they are a luxury that resource-constrained organisations could pursue in the future or perhaps through third-party penetration tester (e.g other cybersecurity consulting company).

## Conclusion

In summary, both the Red Team and Blue Team play a pivotal role in cybersecurity, but their values and responsibilities varies based on organisational context. The Red Team uncover vulnerabilities through offensive simulations, offering insights that strengthen defences. However, their impact is limited without follow-through, and their cost can stain budgets. The Blue team, however, provide continuous defences, incident response, and resilience, making them indispensable for organisations facing daily threats. For an organisation that is only limited to one team, the Blue Team would be a wiser investment. This is because, having a Blue Team establishes a foundation of security that protects against immediate risks, support compliance, and foster long term maturity, ensuring the organisation remains operational and secure in an increasingly hostile digital environment.

## Q3:

The COVID-19 pandemic led to a widespread shift toward remote work, driven by safety concerns and public health restrictions. As a result, home networks became critical components of organisations security. Employees working from home often use personal devices and unsecure networks, significantly increasing the attack surface. As a member of the Red Team, my role is to simulate these attacks with the goal of identifying weaknesses in a home network defence.

In this report, I will outline my approach to testing the security of a typical home network, detailing the objectives and steps involved. Home networks often have vulnerabilities that attackers can exploit, in which in this case could be used to access cooperate systems. By simulating attacks, I aim to uncover risks such as weak network configurations, unpatched devices, and user errors, providing actionable insights to enhance security in this new era of remote work.

## Introduction:

The widespread of the Covid-19 pandemic has reshaped work patters worldwide, with many employees relying on home networks to access cooperate systems. Unlike enterprise environments, home networks often have basic or lack robust security controls, making them a prime target for attackers. Weak Wi-Fi passwords, outdated routers, or even unsecured IoT devices can server as an entry point for attacker to steal sensitive data, or in a worse situation launch broader attacks on corporate systems. A study shown by the tycoon global communication company Verizon, reported that 39% of breaches involved compromised remote access, underscoring the risk of home networks [17, 18].

As a member of the Red Team, my task is to test home network's resilience by simulating attack techniques that would be performed by an unethical hacker. This includes network scanning, phishing, or privilege escalation in order to access the organisations systems. This report defines the objectives and methodology for conducting penetration testing, addressing the unique challenges of home environments.

## Home Security Analysis & Factors Involved:

Home networks present a very distinct security challenges compared to corporate setups. First, they often rely on affordable, consumer grade routers with default or weak credentials, making them vulnerable to brute-force attacks. Secondly, employees may use personal devices (e.g laptops, PC, phones, Tablets) to access corporate systems, lacking endpoint protection, and thus increasing the risk of malware attacks. Thirdly, IoT devices, like smart Tv's or cameras, are common to have unpatched vulnerabilities, as seen in the 2016 Mirai botnet attack, which exploited IoT weaknesses [19].

Furthermore, a common tactic used by cybercriminal is phishing emails, where remote workers commonly fall for such scam, granting attackers access to home systems that connect to corporate VPN's (encrypted connection). The absence of centralized monitoring, unlike in enterprise environments, exacerbates these risks. As a member of the Red Team, I must navigate these issues ethically, ensuring that these tests are authorized and non-disruptive, as outlined in the EC-Council's Code of Ethics.

Another critical issue when it come to working from home, is the overlap between personal and work-related assets. Staff and employees of an organisation working from home may share some networks with family members, introducing variables like guest devices or unsecured gaming consoles (e.g. PlayStation, X-box, PSP, etc). This poses a big challenge, as a penetration tester working as part of a Red Team, I must respect privacy while focusing on work related risks, such as VPN access or corporate data leakage. Despite these obstacles, the main objective here is to simulate realistic threats and provide finding that my organisation could use to secure remote work environments.

## Objectives of The Red Team Assessment:

The primary objective of this Red Team engagement is to evaluate the security posture of home networks used for remote work, with the main emphasis of identifying vulnerabilities that could compromise organisational assets.

It is important to clarify that theses exercise that I am listing below are designed solely to identify weaknesses, not to actively exploit or compromise staff members' home Wi-Fi networks. All testing activities must be conducted strictly within the authorised scope, with proper consent, and in accordance with ethical guidelines, focusing on uncovering possible attack vectors rather than performing real-world intrusions.

This includes the following:

- **Assess staff network configuration:** Determine if the Wi-Fi network uses strong encryption and secure credentials, this also includes checking if the Wi-Fi networks is susceptible to attacks like packet sniffing or credentials cracking.
- **Identify Vulnerable devices:** Detect and report unpatched or misconfigured devices that could be used as an entry point for attackers, this includes routers, laptops, and IoT devices.
- **Test & Report User awareness:** Evaluate the employees' ability to identify and mitigate social engineering tactics, such as phishing, which could lead to unauthorised access to a unknown entity.
- **Inspect Staff Remote Access Tools & VPN Usage:** Its standard practice to check if remote access tools used by staff are properly secured with strong passwords and Multi-Factor Authentication (e.g. Microsoft Authenticator or similar).
- **Identify Weak Segmentation:** Identify and report cases where personal devices, IoT Devices, or smart home systems (e.g. Alexa) share the same networks as the work device.
- **Evaluate Exposure to External Threat Intelligence:** Compare the vulnerabilities identified against know exploits and malware signatures from open-source databases e.g (CVE/NVD), identifying how an attacker could take advantage before they do.
- **Report Data Leakage Risks:** Identify any misconfigured cloud file shares, cloud-syn folders, or local backups that may be exposed to unauthorised access or potential accidental leakage.
- **Provide Actional recommendations & mitigation strategies:** Deliver a report detailing vulnerabilities and mitigation strategies, enabling the organisation to secure remote work setups.

These objectives align with the **NIST 800-115**, which emphasises the simulation of attack reconnaissance and attempting to accesses the organisations system with the main goal of improving security [6]. By performing these tasks mentioned above, the Red Team ensures a comprehensive assessment without disrupting the employees' home environment.

## Steps & Tasks to Test the Home network:

To conduct a thorough Red Team assessment, I will be following a structured methodology, adapting industry-standard penetration testing techniques to the context of home networks. This approach incorporates best practices and knowledge gained from the Penetration Testing Module at the National College of Ireland (NCI), ensuing the assessment is both ethical and effective. The steps outlined below reflect a typical Red Team engagement Lifecycle, specifically tailored to evaluate security posture of remote work environments.

- **Pre-Engagement & Scoping:** Obtain explicit authorisation through a Letter of Engagement, defining the scope and rules of engagement (e.g. Testing VPN access, staff Wi-Fi networks, and laptops). The Letter of Engagement should also specify and confirm in detail the testing window and communication protocols for reporting critical findings. (e.g testing are to be carried out in off work hours). Additionally, a point of contact should also be included in

case of accidental disruption of service, this step ensures compliance with Ireland's legal framework Criminal Justice Act 2017 (Irish Statute Book, 2017) [2, 3].

- **Passive Reconnaissance (Information Gathering):** Collect publicly available information about the home network without direct interaction. Using tools learnt in class, like Shodan and WHOIS to identify exposed devices (mainly routers with open ports) and gather ISP details (Internet Service Provider). Analyse the employee's online presence for potential social engineering vectors, such as LinkedIn profiles revealing job roles, this step although is a bit aggressive, it minimises detection while building a target profile.
- **Active Reconnaissance (Network Scanning):** As mentioned previously, testing is to be conducted with the approval and permission of the involved parties. This includes network scanning using tools like Nmap to map the home network's topology, identifying devices, open ports, and services (e.g. HTTP on port 80 for a router admin panel). Enumerate Wi-Fi details to identify any out-of-date firmware or weak encryption (using tools like Wireshark or Advanced IP Scanner). All testing and results would then be documented and reported to the point of contact (e.g. reporting router out of date firmware which may be vulnerable to known exploits).
- **Vulnerability Assessment:** Analyse the scan results to pinpoint weaknesses. Use tools such as Nessus or OpenVAS to check for CVEs (Common Vulnerabilities and Exposures). Test the Wi-Fi password's strength using tools such as John the Ripper or Hashcat if credentials are obtained ethically (e.g. via authorised disclosure).
- **Simulate an Attack (for the purpose of verifying an Exploitation):** Verify the vulnerabilities discovered by attempting controlled exploitation, this could be achieved by using Metasploit to exploit router's known flaws to access the network. Simulating an attack can also test whether employees can recognise and report suspicious emails or links if social engineering techniques were to be included. This could also allow the Red Team to document behavioural responses, not for blame, but to improve training and organisations policy (All actions are logged to ensure traceability and ethics).
- **Privilege Escalation & Lateral Movement:** In a situation where a member of the Red Team was able to gain access, a test for escalation opportunities, such as exploiting weak user passwords to gain admin rights on routers, should be implemented. Additionally, the security team must check if compromised devices allow lateral movement to other systems, like a work laptop for instance.
- **Report Findings:** Compile a detailed report outlining findings, including vulnerabilities exploited during the attack simulation, attack vectors, and potential impacts (e.g. supported by relevant risk metrics or damage estimates). This report must also include mitigation strategies. Although this is mainly the duty of the Blue Team, including recommended mitigations in the report enhances its value by making it more actionable, informative, and presentable for both technical and non-technical stakeholders.

## Conclusion

As a Red Team member who is conducting penetration testing and assessment of a staff home network, requires a balance of technical expertise, moral and ethical responsibility, as well as adaptability to remote work context. The structured approach outlined above; I can identify critical weaknesses that threaten organisational security (excluding the simulated attack unless approved). The Covid-driven rise in remote work has made home networks a frontline defence, necessitating rigorous testing in order to protect against real world threats. These objectives, not only exposes vulnerabilities, but also solidifies organisations security posture in the context of remote work, ensuring resilience in an increasingly connected environment.

## Q4:

### OpenVAS Vulnerability Report:

#### **Scan details as per the Metasploitable2.pdf report:**

**Host scanned:** 83.212.126.187 - snf-60004.vm.oceanos-global.grnet.gr

**Scan Date:** February 26, 2023

**Start of Scan Time:** Sun Feb 26 20:55:44 2023 UTC

**End of Scan Time:** Sun Feb 26 22:16:26 2023 UTC

**Port assigned** (based on my student number): port 3632

This report details the vulnerabilities identified on port 3632 on the Metasploitable2 system, as per the OpenVAS scan that was initiated on February 26<sup>th</sup>, 2023. Upon a thorough review of the scan results, it was determined that a single, but highly critical, vulnerability is associated with port 3632, specifically affecting the DistCC Daemon (also known as distccd). This vulnerability formally identified and documents as CVE-2004-2687, poses a significant security risk due to its potential to allow unauthorised remote access and arbitrary command execution without the need for authentication.

While there were no additional vulnerabilities detected on port 3632 in the OpenVAS Report, the severity of the vulnerability issue requires immediate attention. Its unauthenticated nature and the level of system compromise it enables, makes it a high priority threat. The following sections present a comprehensive analysis of the vulnerability, informed by extensive research using credible academic and industry sources (google Scholar, NIST, and OWASP top 10). This includes technical details, potential impact, and actionable remediation strategies designed to mitigate associated risks.

## Description:

The DistCC Daemon is a program that distributes builds of programming languages such as C, C++, and many other C languages across several machines within a network, aiming to accelerate the build processes (distributed computing). However, when improperly configured, it can introduce serious security vulnerabilities.

According to the OpenVAS scan conducted on February 26<sup>th</sup>, 2023, the DistCC daemon running on port 3632 of host 83.212.126.187 was found to be vulnerable to a critical remote command execution flaw. This vulnerability, identified as CVE-2004-2687, allows users to execute arbitrary shell commands on the target system. The flaws arise from the systems inability to sanitise user input, in which enables unauthenticated remote attacker to execute arbitrary commands with the privileges of the DistCC process (Root privileges).

The vulnerability was common in DistCC version 2.18.3 which the command would allow you to execute commands typically on the root:

*Figure 1:*(OpenVAS scan result confirming exploitation of the DistCC vulnerability (CVE-2004-2687) on port 3632

#### 2.1.5 High 3632/tcp

High (CVSS: 9.3) NVT: DistCC RCE Vulnerability (CVE-2004-2687)
<b>Summary</b> DistCC is prone to a remote code execution (RCE) vulnerability.
<b>Vulnerability Detection Result</b> It was possible to execute the "id" command. Result: uid=1(daemon) gid=1(daemon)
<b>Impact</b> DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

*Figure 2:* Exploitation of the DistCC vulnerability (CVE-2004-2687) using Metasploit's distcc\_exec module [23].

```
root@bt: /pentest/exploits/framework3
File Edit View Terminal Help
msf exploit(distcc_exec) > show options
Module options (exploit/unix/misc/distcc_exec):
-----
Name      Current Setting  Required  Description
-----
RHOST     metasploitable  yes       The target address
RPORT     3632             yes       The target port

Payload options (cmd/unix/bind_perl):
-----
Name      Current Setting  Required  Description
-----
LPORT     4444             yes       The listen port
RHOST     metasploitable  no        The target address

Exploit target:
-----
Id  Name
--  ---
0   Automatic Target

msf exploit(distcc_exec) > exploit
[*] Started bind handler
whoami
daemon
```

This vulnerability, identified by OpenVAS NVT, serverly compromises the Metasploitable system, which operates on an outdated Ubuntu 8.04 environment with multiple exposed services [20, 21, 22].

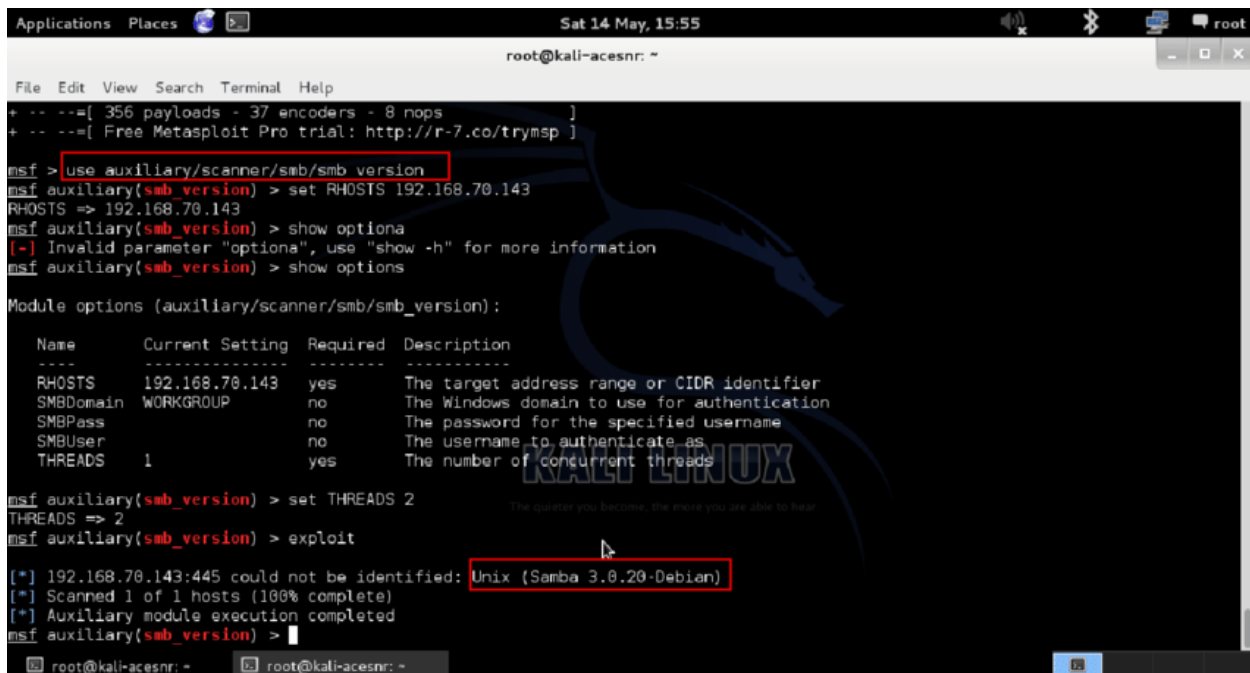


## Impact:

Exploiting this vulnerability could result in the system to be fully compromised, granting attackers root-level access and complete control over the host. This exploit could allow malicious users to breach databases and steal sensitive files or credentials, and can lead to loss of integrity through malware injection or deletion of critical data. Furthermore, attackers may also disrupt services, crash the system, or even exploit other vulnerable services (e.g., Samba, PostgreSQL).

Due to the unauthenticated nature of the DistCC service and its exposure on port 3632, the likelihood of successful exploitation is extremely high. The CVSS score of 9.3 reflects critical severity across all impact vectors, including confidentiality, integrity, and availability.

*Figure 3:* Enumeration of the Samba service running on port 445 of the target machine, using Metasploit. This is a simple example on how an attacker who gains initial access via the DistCC vulnerability on port 3632 could identify and exploit additional services on the same host (Google scholar: Exploiting Vulnerabilities of a Linux Based Machine) [20].



```
Applications Places Sat 14 May, 15:55 root
root@kali-acesnr: ~
File Edit View Search Terminal Help
+ -- ==[ 356 payloads - 37 encoders - 8 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use auxiliary/scanner/smb/smb_version
msf auxiliary(smb_version) > set RHOSTS 192.168.70.143
RHOSTS => 192.168.70.143
msf auxiliary(smb_version) > show options
[-] Invalid parameter "options", use "show -h" for more information
msf auxiliary(smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.70.143  yes       The target address range or CIDR identifier
  SMBDomain WORKGROUP        no        The Windows domain to use for authentication
  SMBPass   [REDACTED]        no        The password for the specified username
  SMBUser   [REDACTED]        no        The username to authenticate as
  THREADS   1                yes       The number of concurrent threads

msf auxiliary(smb_version) > set THREADS 2
THREADS => 2
msf auxiliary(smb_version) > exploit

[*] 192.168.70.143:445 could not be identified: Unix (Samba 3.0.20-Debian)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(smb_version) >
```

**CVSS Breakdown for CVE-2004-2687** (According to National Institute of Standards and Technology, "CVE-2004-2687 - NVD – NIST) [22]:

- **CVSS Bas Score:** 9.3 (Critical)
- **Attack Vector (AV):** Network (AV: N) – It can be exploited remotely over a network
- **Attack Complexity (AC):** Low (AC: L) – There are no special conations that are required for exploitation
- **Authentication:** (Au:N) – The attacker does not require credentials or authentication in any instance to exploit the vulnerability



- **Confidentiality Impact (C):** High (C:H), as attackers can access all sensitive data and across other disrupted systems.
- **Integrity Impact:** High (I:H), as it allows the attacker to modify and delete system data
- **Availability Impact (A):** High, as the attacker can disrupt the service, e.g DDoS attack or crashing the system.

## Recommended Remedial Measures:

To mitigate the DistCCDaemon Command Execution Vulnerability (CVE-2004-2687) that was identified on port 3632, the following remediation steps are recommended. These steps are guided by industry best practices and aligns with NIST vulnerability management standards and OWASP top 10 [23 ,25 ,27].

- **Disable the DistCC service:** If the DistCC service is no longer required, it is recommended to stop and disable the service entirely using the “systemctl” command line utility (e.g “systemctl stop distcc” & “systemctl disable distcc”). This should be done immediately as this eliminates the attack vector entirely.
- **Upgrade DistCC (VendorFix):** This was recommended in the attached openvas-metasploitable2 pdf report, updated version of DistCC which includes patches for address the unauthenticated execution flaw.
- **Restrict Network Access & Enforce Authentication:** According to DistCC security notes, older versions of DistCC do not enforce must use the “—allow” rule and or firewall rules to limit access to the port since arbitrary commands can be executed (3.0 and above versions of DistCC reinforce this). Additionally, DistCC must be configured to only allow authorised clients, although this might not be enough, DistCC security note suggest using SSH policies [24].
- **Least Privileges Principles:** Since this vulnerability was exploited using root access, the daemon should run under a non-root user with minimal privileges to reduce the potential impact of the vulnerability.
- **Implement IDS systems & Regular patch updates:** Deploy intrusion detection systems (IDS) like Snort (or equivalent) to monitor activity on the target port for any signs of exploitation attempts. Performing frequent vulnerability scans with tools like OpenVAS is highly recommended, as this can identify any unpatched services and apply updates accordingly (OWASP Secure Coding Practices / Security Misconfiguration) [25, 26].
- **Security Awareness and Configuration Review:** Staff and administrators should receive training on the risks associated with exposed development services. Proper configuration hardening is crucial, especially in testing environments like Metasploitable2 as shown in Figure 3. The attached OpenVAS report has also confirmed successful command execution using the “id” command on the vulnerable system (Figure 1), this emphasises the ease of which the attacker can compromise exposed service [26, 27]. Additional guidance on secure configurations and awareness training can be found in the [OWASP Testing Guide: Configuration Management](#) and [NIST Guide to General Server Hardening](#).)

## References:

- [1]  
EC-Council, “Code Of Ethics - EC-Council,” *EC-Council*. <https://www.eccouncil.org/code-of-ethics/>
- [2]  
K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, “Technical Guide to Information Security Testing and Assessment,” *csrc.nist.gov*, Sep. 30, 2008. <https://csrc.nist.gov/pubs/sp/800/115/final>
- [3]  
electronic I. S. Book (eISB), “electronic Irish Statute Book (eISB),” *www.irishstatutebook.ie*. <https://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/html>
- [4]  
The Crown Prosecution Service, “Computer Misuse Act,” *www.cps.gov.uk*, Feb. 05, 2020. <https://www.cps.gov.uk/legal-guidance/computer-misuse-act>
- [5]  
EC-Council, “Code Of Ethics | CERT,” *cert.eccouncil.org*. <https://cert.eccouncil.org/code-of-ethics.html>
- [6]  
“NIST SP 800-115 and Penetration Testing,” *www.softwaresecured.com*. <https://www.softwaresecured.com/post/nist-sp-800-115-and-penetration-testing>
- [7]  
K. Scarfone, Murugiah Souppaya, A. Cody, and A. Orebaugh, “NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment,” Sep. 29, 2008. [https://www.researchgate.net/publication/329973439\\_NIST\\_Special\\_Publication\\_800-115\\_Technical\\_Guide\\_to\\_Information\\_Security\\_Testing\\_and\\_Assessment](https://www.researchgate.net/publication/329973439_NIST_Special_Publication_800-115_Technical_Guide_to_Information_Security_Testing_and_Assessment)
- [8]  
Bharat Kotwani, Miss Rohini Sawant, and Dr Shalu Chopra, “Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield,” *INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT*, vol. 07, no. 12, pp. 1–11, Dec. 2023, doi: <https://doi.org/10.55041/ijssrem27675>.
- [9]  
“Certified Network Defender (CND) | Network Security Course,” *EC-Council*. <https://www.eccouncil.org/train-certify/certified-network-security-course/>
- [10]  
IBM, “Blue Team,” *Ibm.com*, Dec. 18, 2023. <https://www.ibm.com/think/topics/blue-team> (accessed Apr. 9, 2025).

[11]

Verizon, “DBIR 2023 Data Breach Investigations Report Public Sector Snapshot,” 2023. Available: <https://www.verizon.com/business/resources/Ta5a/reports/2023-dbir-public-sector-snapshot.pdf>

[12]

J. Cranford, “Red Team VS Blue Team: What’s the Difference? | CrowdStrike,” *CrowdStrike.com*, 2019. <https://www.crowdstrike.com/en-us/cybersecurity-101/advisory-services/red-team-vs-blue-team/>

[13]

Aleksandra Velickovic, “Red Team vs Blue Team in Cyber Security: Threat Intelligence 101,” *Capaciteam*, Apr. 05, 2024. <https://capaciteam.com/red-team-vs-blue-team-cyber-security-101/> (accessed Apr. 10, 2025).

[14]

Orani Amroussi, “IBM’s Cost of a Data Breach 2024: What we learned,” *Vulcan Cyber*, Sep. 05, 2024. <https://vulcan.io/blog/ibm-cost-of-a-data-breach-2024> (accessed Apr. 10, 2025).

[15]

“2025 Cost of Insider Risks: Takeaways From Ponemon’s Largest Insider Threat Study Yet,” *DTEX Systems*, Mar. 14, 2025. <https://www.dtexsystems.com/blog/2025-cost-insider-risks-takeaways/>

[16]

Okan Yıldız, “Mastering Blue Teaming: An Exhaustive Guide to Defensive Cybersecurity Operations,” *Medium*, Nov. 23, 2024. <https://medium.com/@okanyildiz1994/mastering-blue-teaming-an-exhaustive-guide-to-defensive-cybersecurity-operations-1587f0ca8c54>

[17]

“85% of Data Breaches Involve Human Interaction: Verizon DBIR,” *www.darkreading.com*. <https://www.darkreading.com/cybersecurity-operations/85-of-data-breaches-involve-human-interaction-verizon-dbir>

[18]

“Verizon: Healthcare Phishing and Ransomware Attacks Increase while Insider Breaches Fall,” *HIPAA Journal*, May 14, 2021. <https://www.hipaajournal.com/verizon-healthcare-phishing-and-ransomware-attacks-increase-while-insider-breaches-fall/>

[19]

Cloudflare, “What is the Mirai Botnet?,” *Cloudflare*, 2025. Available: <https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/>

[20]

Imrana Abdullahi Yari, “Exploiting Vulnerabilities of a Linux Based Machine: Penetration Testing Report and Incident Response Procedure,” Sep. 01, 2016.  
[https://www.researchgate.net/publication/352102901\\_Exploiting\\_Vulnerabilities\\_of\\_a\\_Linux\\_Based\\_Machine\\_Penetration\\_Testing\\_Report\\_and\\_Incident\\_Response\\_Procedure?channel=doi&linkId=60b9040c92851cb13d73f593&showFulltext=true](https://www.researchgate.net/publication/352102901_Exploiting_Vulnerabilities_of_a_Linux_Based_Machine_Penetration_Testing_Report_and_Incident_Response_Procedure?channel=doi&linkId=60b9040c92851cb13d73f593&showFulltext=true)

[21]

“OpenVas Vulnerability Report.” Available: <https://hackertarget.com/sample-vulnerability-report/metasploitable-2.0-openvas.pdf>

[22]

“NVD - CVE-2004-2687,” *nvd.nist.gov*. <https://nvd.nist.gov/vuln/detail/CVE-2004-2687>

Figure 2 image source: [23]

Marcin Teodorczyk, “Understanding Privilege Escalation» ADMIN Magazine,” *ADMIN Magazine*, 2025. [https://www.admin-magazine.com/Articles/Understanding-Privilege-Escalation/\(offset\)/2](https://www.admin-magazine.com/Articles/Understanding-Privilege-Escalation/(offset)/2) (accessed Apr. 12, 2025).

[23]

NIST, “Security and Privacy Controls for Information Systems and Organizations,” *csrc.nist.gov*, Sep. 2020. <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

[24]

“distcc security notes,” *www.distcc.org*. <https://www.distcc.org/security.html>

[25]

OWASP, “OWASP Secure Coding Practices - Quick Reference Guide | Secure Coding Practices | OWASP Foundation,” *owasp.org*, 2024. <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist>

[26]

OWASP, “A6:2017-Security Misconfiguration | OWASP,” *owasp.org*, 2017.  
[https://owasp.org/www-project-top-ten/2017/A6\\_2017-Security\\_Misconfiguration](https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration)

[27]

“WSTG - Latest | OWASP Foundation,” *owasp.org*. [https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/02-Configuration\\_and\\_Deployment\\_Management\\_Testing/README](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/README)