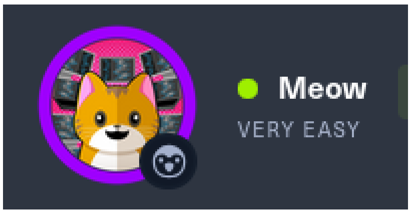
REPORT MEOW HTB



CONFIDENTIALITY NOTICE

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to HTB or facilitate attacks against HTB. Jonas Fernandez shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

DISCLAIMER

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on HTB’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.

EXECUTIVE SUMMARY

On May 18, 2025, Jonas Fernandez performed a security assessment of HTB’s internal corporate network. With decades of combined cybersecurity experience, our team simulated an external threat actor attempting to gain unauthorized access to systems within HTB’s infrastructure. The objective was to uncover vulnerabilities and recommend appropriate remediation measures to enhance the network's security posture.

During the assessment, a single vulnerability was identified—rated as **High** severity:

HIGH
1

The identified vulnerability was found in the configuration of the Telnet service. Specifically, Telnet was running on port 23 and allowed direct login as the root user by accepting blank credentials. Although this vulnerability is categorized as high rather than critical in our assessment, the risk remains significant. The flaw essentially permits an attacker to bypass authentication, potentially gaining administrative access to the system. Moreover, Telnet transmits all data in plaintext, exposing sensitive communications to interception.

Given these risks, it is highly recommended that HTB immediately remediate this vulnerability by securing remote access channels. Transitioning from Telnet to a more secure protocol such as SSH, enforcing robust password policies, and thoroughly reviewing remote service configurations are essential actions to protect the confidentiality, integrity, and availability of critical systems.

Please note that this assessment may not disclose every vulnerability that exists in the environment, and any environmental changes during testing may affect the results.

HIGH LEVEL ASSESSMENT OVERVIEW

Observed Security Strengths

Jonas Fernandez identified several strengths within **HTB**’s network that contribute positively to its overall security posture. These strengths include:

- **Effective Network Segmentation:** The internal network is segmented in a way that limits direct exposure of critical systems to potential external threats.
- **Regular Security Maintenance:** Periodic internal audits suggest that some attention is already given to maintaining basic security hygiene across the network.

Maintaining and further developing these controls will be essential to uphold and enhance the network's security over time.

Areas for Improvement

Jonas Fernandez recommends that **HTB** adopts the following improvements to strengthen the security of its network. Addressing these issues will significantly reduce the risk of successful attacks and minimize the potential impact should an exploitation occur.

Short Term Recommendations

To immediately reduce business risk, **Jonas Fernandez** advises **HTB** to take the following actions as soon as possible:

- **Immediate Deactivation or Replacement of Telnet:** The assessment revealed a high-severity vulnerability in the Telnet service—running on port 23—which permits direct login as the root user via blank credentials. This configuration allows an attacker to bypass authentication entirely and access the system with full administrative privileges. It is critical to disable Telnet on all systems in favor of a secure alternative, such as SSH, which offers robust encryption and authentication mechanisms.
- **Removal of Blank Credentials:** Secure all administrative accounts by enforcing strong, unique passwords. Eliminate any reliance on default or empty credentials, especially on high-privilege accounts.
- **Enhance Basic Access Control Measures:** Reinforce authentication strategies by incorporating multi-factor authentication (MFA) where applicable and restricting remote access to only authorized users.

Long Term Recommendations

For sustainable security improvements, **Jonas Fernandez** recommends that **HTB** implements the following actions over the coming months:

- **Comprehensive Audit of Remote Access Protocols:** Conduct an in-depth review of all remote access points (not only Telnet) to ensure that legacy protocols are either upgraded to modern, secure alternatives or completely removed from the environment.
- **Ongoing Configuration Management and Hardening:** Establish and enforce automated processes to monitor and review system configurations regularly. This policy should include baseline configuration standards that prevent insecure settings and ensure that all services are consistently harden against known vulnerabilities.

- **Enhanced Security Awareness and Training:** Implement continuous training programs for IT personnel focusing on secure configuration management, the identification of vulnerabilities, and best practices in remediation to maintain a proactive security culture.

SCOPE

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

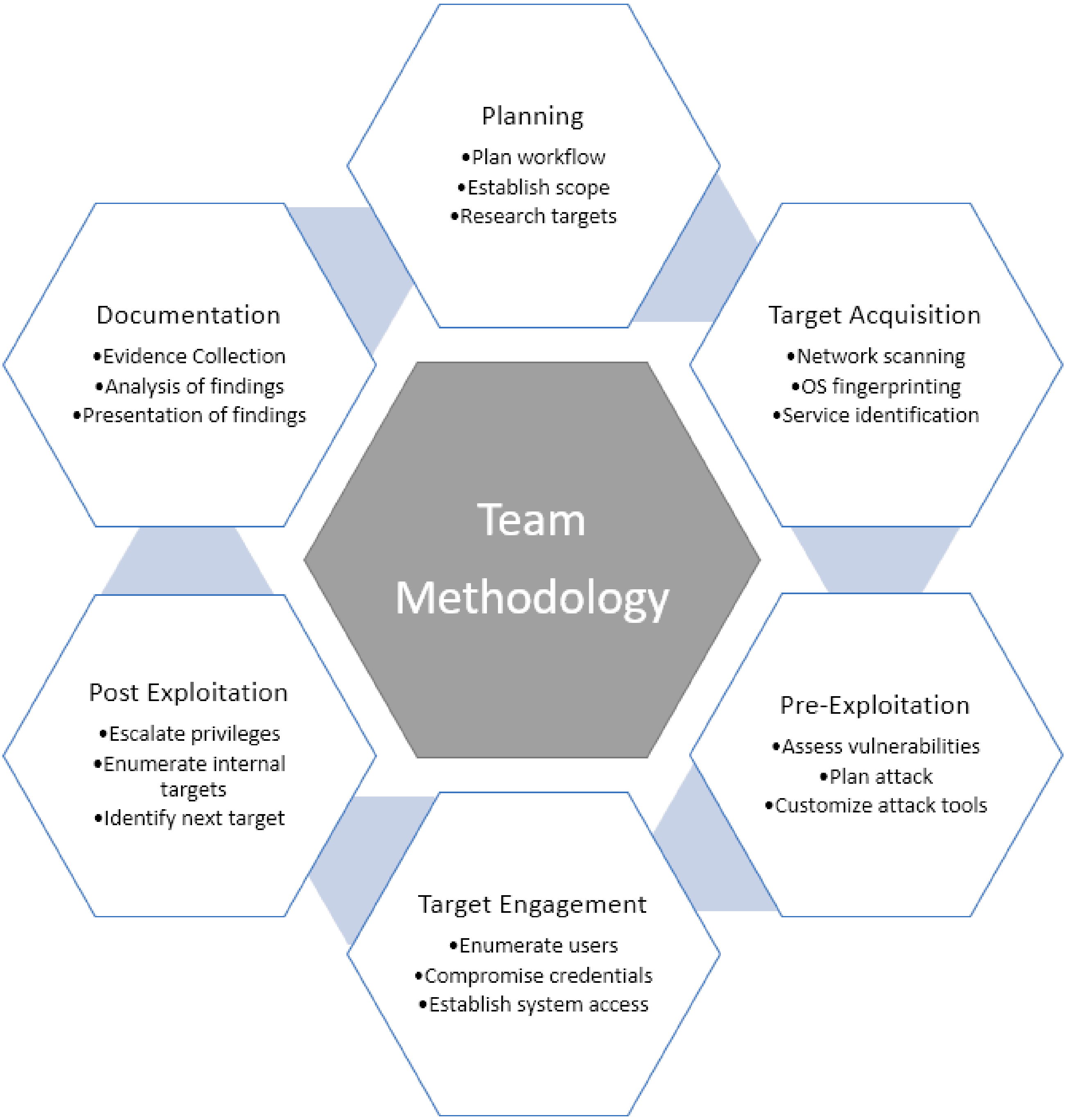
Host

Host	Note
10.129.84.91	Meow

TESTING METHODOLOGY

Jonas Fernandez's testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about HTB's network systems. Jonas Fernandez used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. Jonas Fernandez simulated an attacker exploiting vulnerabilities in the HTB network. Jonas Fernandez gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.



CLASSIFICATION DEFINITIONS

Risk Classifications

Level	Score	Description
Critical	**10**	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	**7-9**	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.

Level	Score	Description
Medium	**4-6**	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	**1-3**	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Informational	**0**	These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company.

Exploitation Likelihood Classifications

Likelihood	Description
Likely	Exploitation methods are well-known and can be performed using publicly available tools. Low-skilled attackers and automated tools could successfully exploit the vulnerability with minimal difficulty.
Possible	Exploitation methods are well-known, may be performed using public tools, but require configuration. An understanding of the underlying system is necessary for successful exploitation.
Unlikely	Exploitation requires a deep understanding of the underlying systems or advanced technical skills. Precise conditions may be required for successful exploitation.

Business Impact Classifications

Impact	Description
Major	Successful exploitation may result in large disruptions of critical business functions across the organization and significant financial damage.
Moderate	Successful exploitation may cause significant disruptions to non-critical business functions.
Minor	Successful exploitation may affect few users, without causing much disruption to routine business functions.

Remediation Difficulty Classifications

Difficulty	Description
Hard	Remediation may require extensive reconfiguration of underlying systems that is time consuming. Remediation may require disruption of normal business functions.
Moderate	Remediation may require minor reconfigurations or additions that may be time-intensive or expensive.
Easy	Remediation can be accomplished in a short amount of time, with little difficulty.

ASSESSMENT FINDINGS

Number	Finding	Risk Score	Risk	Page
1	**Telnet CWE-798 Unauthorized Root Access** (Blank credentials enable direct root login)	9.4	**High**	N/A

Telnet CWE-798

1. Initial Port Scan We began by scanning the target to identify active services. The initial Nmap scan revealed that the Telnet service was running on port 23 and was open. The output below confirms these details:

```
kali@kali ~/workspace/machines/meow [07:29:26] $ cat allports
# Nmap 7.95 scan initiated Sun May 18 06:52:09 2025 as: /usr/lib/nmap/nmap
-sS -p- --open -n -Pn --min-rate 5000 -oN allports 10.129.84.91
Nmap scan report for 10.129.X.X
Host is up (0.035s latency).
Not shown: 60619 closed tcp ports (reset), 4915 filtered tcp ports (no-
response)
Some closed ports may be reported as filtered due to --defeat-rst-
ratelimit
PORT   STATE SERVICE
23/tcp open  telnet

# Nmap done at Sun May 18 06:52:20 2025 -- 1 IP address (1 host up)
scanned in 11.04 seconds
```

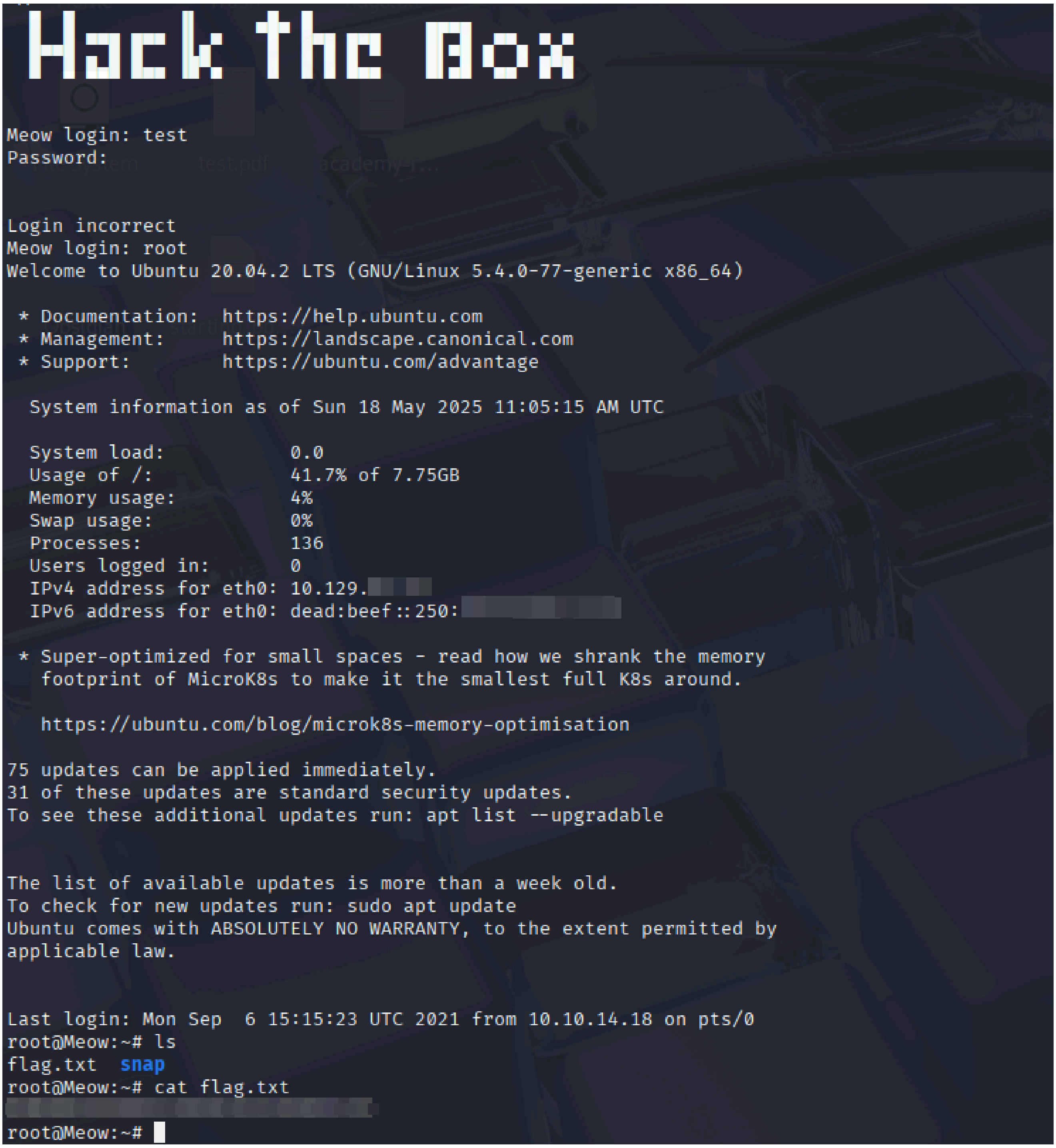
2. Service Enumeration and Version Detection Next, we performed a targeted scan to gather further details about the Telnet service. This scan provided additional information, confirming that the service is running as **Linux telnetd** on a Linux host. The following output illustrates the results:

```
kali@kali ~/workspace/machines/meow [07:29:34] $ cat targeted
# Nmap 7.95 scan initiated Sun May 18 07:02:48 2025 as: /usr/lib/nmap/nmap
-sCV -p 23 -oN targeted 10.129.X.X
Nmap scan report for 10.129.84.91
Host is up (0.056s latency).

PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun May 18 07:03:10 2025 -- 1 IP address (1 host up)
scanned in 22.80 seconds
```

We can retrieve additional information from here, the host is Linux and the version is "Linux telnetd"

3. Authentication Bypass and Root Access The critical vulnerability emerged when confirming that the Telnet service allowed access with blank credentials. The misconfiguration enabled us to log in directly as **root**, bypassing any authentication mechanism. The ability to connect as the root user, with no credentials required, represents a severe security flaw. This was verified with the following command:

```
kali@kali > telnet 10.129.x.x
```



```
Hack the Box

Meow login: test
Password:


Login incorrect
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 18 May 2025 11:05:15 AM UTC

  System load:             0.0
  Usage of /:              41.7% of 7.75GB
  Memory usage:            4%
  Swap usage:              0%
  Processes:               136
  Users logged in:         0
  IPv4 address for eth0:   10.129.[redacted]
  IPv6 address for eth0:   dead:beef::250:[redacted]

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
root@Meow:~# cat flag.txt
[redacted]
root@Meow:~# 
```

4. Summary This exploitation path demonstrates a multi-step process wherein the target's Telnet service is first discovered and enumerated, followed by a verification of its insecure configuration. The severity is dramatically underscored by the fact that we were able to connect as **root**—an administrative level account—without any authentication. This not only exposes the system to complete control by an attacker but also compromises the confidentiality, integrity, and availability of the environment.

Recommendations

- **Disable Telnet Service:**
  Immediately disable the Telnet service and replace it with a secure alternative (e.g., SSH). This ensures that remote communications are encrypted and reduces the risk of unauthorized access.

- **Eliminate Blank Credentials:**
  Remove any default or blank credentials—particularly for the root account—by enforcing strong, unique passwords.
- **Enhance Access Controls:**
  Implement stricter access controls by:
  - Restricting remote access to only trusted IP ranges.
  - Incorporating multi-factor authentication where possible.
  - Regularly reviewing firewall rules and access policies.
- **Implement Regular Audits:**
  Ensure continuous monitoring and periodic audits of remote access configurations and administrative accounts to detect any future misconfigurations or vulnerabilities.

APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
Nmap	Used for scanning ports on the target host (10.129.84.91, "Meow") and identifying open services, such as Telnet on port 23.
Telnet	Used to connect directly to the Telnet service to test the vulnerability (unauthorized root access with blank credentials) on the target host.
Kali Linux	The operating system used as the primary testing platform for conducting this security assessment.
OpenVPN	Used to establish a secure connection to the internal corporate network, allowing remote access during the testing process.

APPENDIX B - ENGAGEMENT INFORMATION

Client Information

- **Client:** HTB
  (This report corresponds to the HTB lab, where the vulnerability assessment was conducted on the "Meow" machine.)
- **Primary Contact:**
  HTB Lab Administrator
  (Since this is a test environment, this entry serves as the in-house point of contact.)
- **Approvers:**
  - John Doe *(Placeholder)*
  - Jane Smith *(Placeholder)*
    (In a real engagement, these would be the individuals authorized to modify the scope or terms of the engagement. In this lab context, they are provided as examples.)

Version Information

Version	Date	Description
1.0	2025-05-18	Initial report to the client

Contact Information

- **Name:** Jonas Fernandez – Independent Penetration Tester
- **Address:** 1001 Fake Street, Gotham, NY 11201
- **Phone:** 555-185-1782
- **Email:** jonas.fernandez@example.com