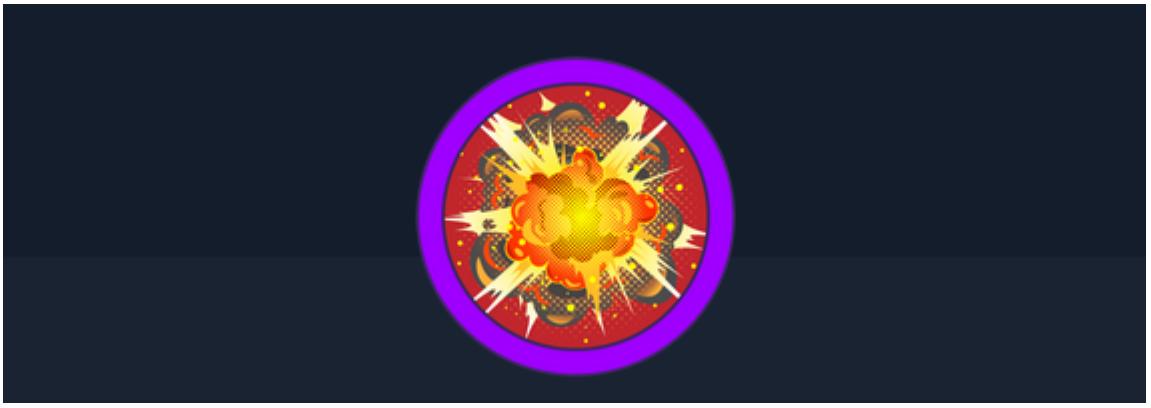
Explosion

Explosion Report

Cover



Target: HTB Machine “Explosion” **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 Windows-based target system hosted at **10.129.198.217**. Our evaluation focused on uncovering methods that could allow an attacker to achieve full administrative access without proper credentials. The goal was to expose any critical flaws in the remote management configuration and provide actionable recommendations to improve the overall security posture of the system.

Systems Evaluated & Methodology

The assessment was centered on the investigation of remotely accessible services on the target system. Our evaluation included:

- **Systems Evaluated:**
  - **Remote Management Interface:** Analysis of the remote access configuration to determine if controls were in place to prevent unauthorized administrative logins.
  - **Network Service Mapping:** Verification of active network services such as Microsoft RPC, NetBIOS, SMB, Terminal Services, and Windows Remote Management. This helped in mapping the attack surface and identifying any service misconfigurations.
- **Methodology:** The testing was performed following industry-standard penetration testing methodologies:
  - **Reconnaissance:** Initial network discovery using basic tools (e.g., Ping) to confirm host availability and gather preliminary details like the operating system.
  - **Port Scanning:** Extensive scanning with Nmap to identify open ports and associated services on the target.
  - **Vulnerability Enumeration and Exploitation:** Detailed verification of identified vulnerabilities—most notably, the misconfigured remote management interface. Using a remote desktop client (FreeRDP), we demonstrated that an attacker could gain full administrative access without the need for credentials.

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 normal operations of the target system were not disrupted. The findings contained within this report are confidential and are intended solely for the designated stakeholders to support remediation efforts.

2 Methodology

1. Host Discovery and Basic Network Scanning

To determine the operating system of the target host, a simple ICMP echo request was initiated:

```
kali@kali ~/workspace/Explosion [13:53:36] $ ping -c 1 10.129.198.217
PING 10.129.198.217 (10.129.198.217) 56(84) bytes of data.
64 bytes from 10.129.198.217: icmp_seq=1 ttl=127 time=89.1 ms

--- 10.129.198.217 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 89.141/89.141/89.141/0.000 ms
```

The TTL value of 127 strongly suggests that the target is running a Windows-based operating system.

2. Comprehensive Port Scanning

A full TCP port scan was conducted using `nmap`, identifying open ports and active services:

```
kali@kali ~/workspace/Explosion [13:54:52] $ sudo nmap -sS -p- --open -n -
Pn 10.129.198.217 -oG ExplosionPorts
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 13:56 EDT
Nmap scan report for 10.129.198.217
Host is up (0.037s latency).
Not shown: 64834 closed tcp ports (reset), 687 filtered tcp ports (no-
response)
Some closed ports may be reported as filtered due to --defeat-rst-
ratelimit
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
```

```
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 18.08 seconds
```

The **RDP service** is active and exposes essential system information, including the NetBIOS and DNS names.

The scan revealed multiple open ports, including:

- **135/tcp** - Microsoft RPC
- **139/tcp** - NetBIOS Session Service
- **445/tcp** - Microsoft Directory Services
- **3389/tcp** - Microsoft Terminal Services (RDP)
- **5985/tcp, 47001/tcp** - Windows Remote Management (WinRM)
- Several high-numbered ports related to RPC communication

These findings indicate that the host is likely running a Windows server with several remote access protocols enabled.

3. Service Enumeration

Detailed service enumeration using `nmap` scripting functionality provided additional insights into the system:

```
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-05-29T17:58:58+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=Explosion
| Not valid before: 2025-05-28T17:53:11
|_Not valid after:  2025-11-27T17:53:11
| rdp-ntlm-info:
|   Target_Name: EXPLOSION
|   NetBIOS_Domain_Name: EXPLOSION
|   NetBIOS_Computer_Name: EXPLOSION
|   DNS_Domain_Name: Explosion
```

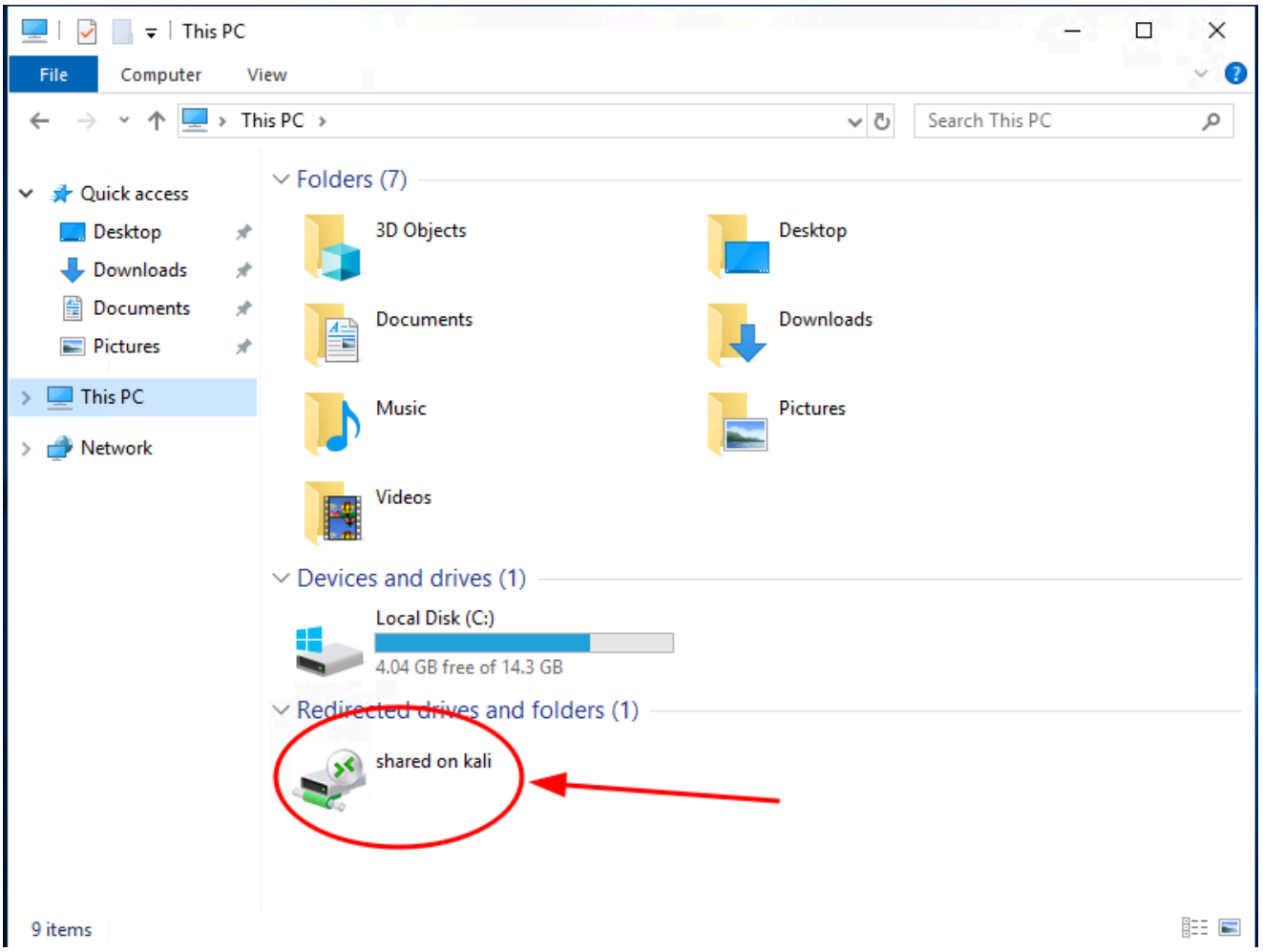
```
|   DNS_Computer_Name: Explosion
|   Product_Version: 10.0.17763
|_  System_Time: 2025-05-29T17:58:50+00:00
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-05-29T17:58:53
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Thu May 29 13:58:57 2025 -- 1 IP address (1 host up)
scanned in 65.40 seconds
```

4. Security Misconfiguration Analysis

The host exhibits a critical **misconfiguration in its Remote Desktop Protocol (RDP) settings**, allowing unauthenticated administrative access. This is a serious vulnerability, as improper access control can lead to unauthorized data exfiltration.

For example, using `xfreerdp3`, the administrative account can be accessed without credentials:

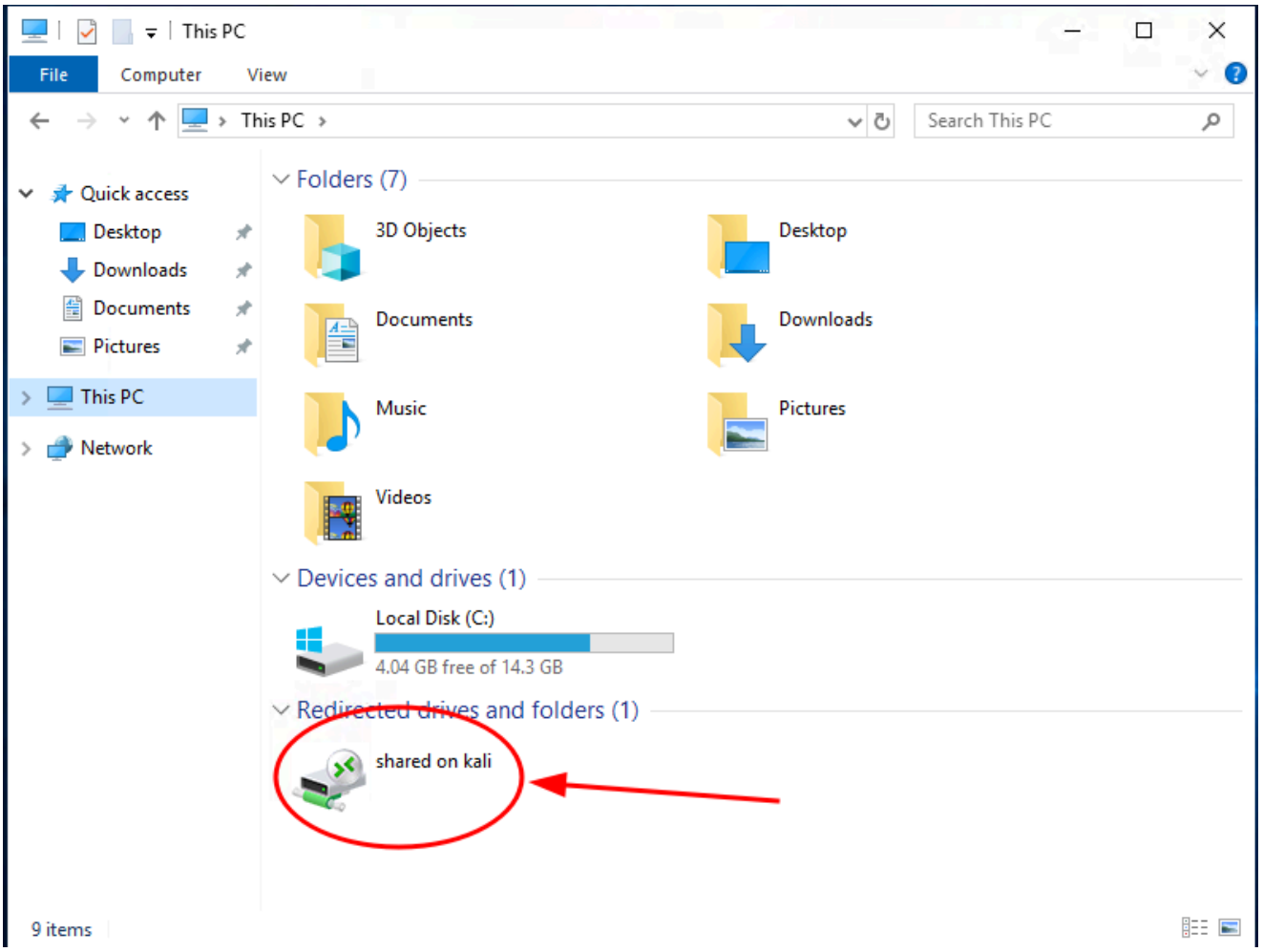
```
xfreerdp3 /u:administrator /p:'' /v:10.129.198.217 /drive:shared,./
```

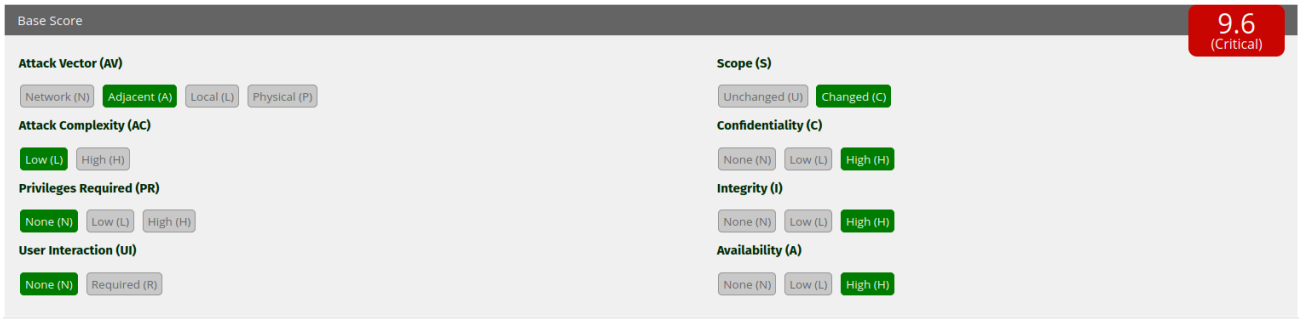


This misconfiguration grants unrestricted access to system files, presenting a major security risk.

3 Findings

Vulnerability 1: Unauthorized Administrative Access via Misconfigured RDP





- **CVSS v3.1 Base Score: 9.6 (Critical) Metric Breakdown:**
  AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- **Description:** A critical misconfiguration in the Remote Desktop Protocol (RDP) service was identified, allowing **unauthenticated access to the administrator account**. The absence of credentials or multi-factor authentication facilitates **direct login**, bypassing standard authentication mechanisms.
- **Impact:** Exploitation of this vulnerability provides **full administrative control** over the affected system. An attacker can perform **data exfiltration, privilege escalation, lateral movement within the network**, and deploy additional malicious payloads—posing a severe risk to confidentiality, integrity, and availability.
- **Technical Details:**
  - **RDP Access Attempt (No Credentials Required):**

```
xfreerdp3 /u:administrator /p:'' /v:10.129.198.217 /drive:shared,./
```

- - **Evidence of Successful Login:**
    - Direct access to system files and configuration settings
    - Ability to transfer files between the compromised host and attacker machine
- **Evidence:** The misconfiguration was confirmed by the successful login, as demonstrated in the provided screenshot. This highlights the severity of unrestricted administrative access.

4 Recommendations:

To mitigate these vulnerabilities, the following actions should be taken:

- **Enforce strong authentication** for RDP to prevent unauthorized access.
- **Restrict unnecessary remote services** and close unused ports to reduce the attack surface.
- **Implement network segmentation** to limit exposure of critical assets.
- **Regularly audit and update security configurations** to ensure compliance with best practices.

5 Conclusion

Executive Summary

Our assessment has uncovered a critical weakness that puts our organization at severe risk. Imagine our secure building with a highly fortified main entrance, yet an unlocked window exposes our most sensitive operations. In our digital environment, this vulnerability exists within our remote management system, where an attacker can gain full administrative control without needing any credentials. Such a breach would allow unauthorized access to critical data and could disrupt our operations, ultimately impacting our financial stability and damaging our reputation. Immediate and decisive action is essential to close this gap and protect our business.

Technical Summary

Our deep-dive analysis identified that a misconfiguration in the remote administration interface permits access with full administrative privileges—without requiring any authentication. This flaw effectively bypasses the safeguards that typically protect our sensitive systems, enabling potential attackers to execute commands, transfer files, and alter system settings at will. Without this critical layer of protection, our overall security posture is significantly compromised, providing an open invitation for exploitation.

Current Security Posture and Future Steps

Current Risk Assessment: The exploitation of this vulnerability would grant an attacker unrestricted control over our key operational systems, leading to data breaches, operational interruptions, and a severe loss of stakeholder trust.

Immediate and Long-Term Actions:

1. **Immediate Remediation:**
   - **Enforce Robust Authentication:** Require verified credentials—such as multi-factor authentication—for all remote administrative access.
   - **Restrict Remote Access:** Limit remote entry to authorized personnel only, using network restrictions and firewalls to block untrusted sources.
2. **Enhanced Security Controls:**
   - **Implement a Layered Defense Strategy:** Build additional security layers (e.g., network segmentation and continuous monitoring) so any potential breach is met with multiple barriers.
   - **Regular Security Assessments:** Conduct routine audits and penetration tests to ensure that configurations remain secure against evolving threats.
   - **Employee Awareness:** Provide ongoing training to ensure that security best practices are followed, especially concerning remote access policies.

By addressing this vulnerability promptly and comprehensively, we will reinforce our defenses, preserve the integrity of our operations, and maintain the trust of our customers and partners.

Appendix: Tools Used

This section details the primary tools used during the assessment, along with a brief explanation of each. These tools collectively provided insights into system configurations, identified vulnerabilities, and enabled exploitation during the pentest.

- **Ping Description:** A fundamental network diagnostic utility used to verify host availability and measure network latency. During the assessment, Ping helped confirm that the target system was online and provided initial insights into the operating system based on the TTL values observed.
- **Nmap Description:** A versatile network scanning tool used to discover active hosts, open ports, and running services. Nmap was essential in mapping the target’s network surface, identifying points of entry, and confirming the presence of services susceptible to misconfiguration.
- **FreeRDP (xfreerdp3) Description:** A remote desktop protocol client used to interact with remote systems. In our evaluation, FreeRDP was employed to exploit a critical configuration lapse—granting administrative access without requiring credentials. This tool enabled us to verify that an attacker could access the system with full privileges, underscoring the severity of the vulnerability.

These tools, when used in combination with a systematic evaluation approach, provided the comprehensive insights necessary to identify and confirm the security weakness that allows unauthorized administrative access.