|  |  |  |
| --- | --- | --- |
| PENETRATION TESTING REPORT | | |
|  |  |  |
| CMF Company  FRIDAY 14TH JUNE 2024 | | |
| DISCLAIMER  This report is to identify vulnerabilities within the specified scope. It contains sensitive information and must be kept confidential. The provider denies liability for damages. The reader is responsible for remediation and maintaining security measures. Contact a higher power for details. | | |

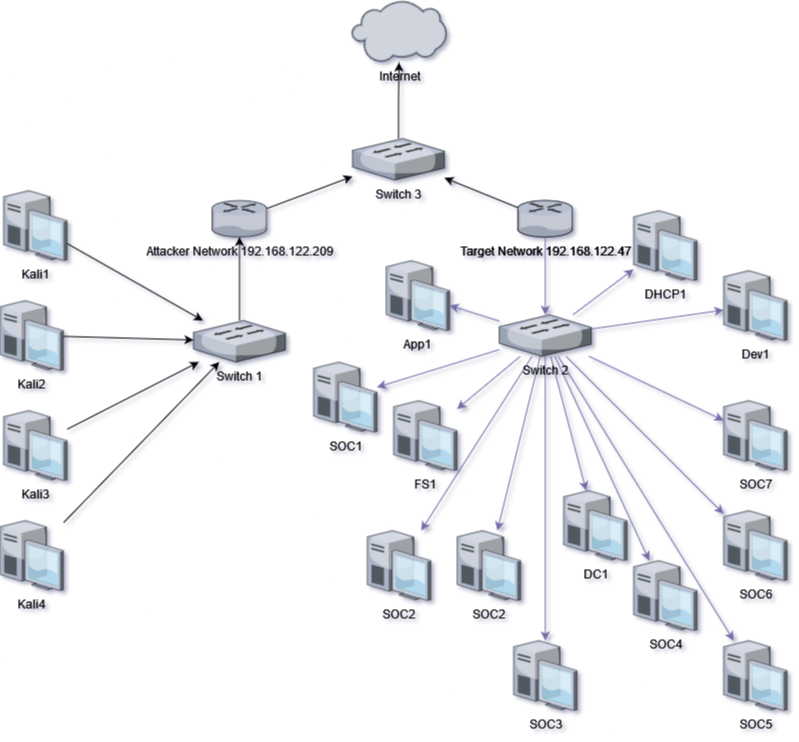
This penetration testing report has been produced in partial fulfillment of the requirements of contract #2024-04-CPPT-WDX. It details the results of the penetration testing engagement conducted from 10 June 2024 to 14 June 2024. This report's contents have an overall confidential classification and are protected by a non-disclosure agreement pursuant to the said contract's requirements.

Tester: CHASTITY ALLEN, FARRUKH KHAN, MERCY OSUGO

Supervisor: LOGAN HILLARD

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **TABLE OF CONTENTS** |   Network Topology 3  1. Executive Summary 4  2. Finding Summary 5  3. Significant Findings 7  4. Flags 17 |

|  |
| --- |
| NETWORK TOPOLOGY |



|  |
| --- |
| Executive Summary |

### 1.1 RESULTS

The technical risks of the systems/network within scope have been assessed as: CRITICAL. This may be mitigated to a residual risk less than HIGH if all remediation recommendations detailed in Section 3 of this report are followed. Consequently, we assess the application/system/network as NOT sufficiently resilient for the production/live environment.

### 1.2 METHODOLOGY

The security evaluation of PLC network consisted of a penetration test, following a grey box approach. This testing was based on recognized methodologies, such as OWASP Testing Guide, OSSTMM and PTES.

### 1.3 SCOPE

This security evaluation was executed from 10-06-2024 to 14-06-2024 and was limited to the review of due to time constraints:

1. 192.168.1.121
2. 192.168.1.109

The following items/components were not tested:

* VPN Server
* Router/switches within the LAN

### 1.4 TECHNICAL ISSUES

No technical issues were encountered during the review. We would like to acknowledge the outstanding support of Farrukh Khan, Chastity Allen and Mercy Osugo.

|  |
| --- |
| 2 Finding Summary |

The penetration test identified two critical Remote Code Execution (RCE) vulnerabilities that allow attackers to execute arbitrary code and potentially gain remote control over affected systems. These vulnerabilities are summarized below:

1. **Web Application RCE (CVE-2024-0001)**:
   * **Description**: A critical RCE vulnerability was found in the general functionality of the web application. This flaw allows attackers to execute arbitrary code, leading to a reverse shell and giving them remote control over the server.
   * **Affected Systems**: The general functionality of the web application.
   * **Recommendations**: Implement stringent input validation and sanitization, employ security measures such as Web Application Firewalls (WAF) and conduct thorough code reviews.
2. **Webmin RCE (CVE-2024-0002)**:
   * **Description**: A critical RCE vulnerability was identified in Webmin, the web-based system administration interface. This vulnerability enables attackers to execute arbitrary commands on the server, potentially resulting in a reverse shell and providing remote control over the server.
   * **Affected Systems**: The Webmin service, particularly its admin interface.
   * **Recommendations**: Update Webmin to the latest version, restrict access to trusted IP addresses, implement strong authentication mechanisms, and regularly monitor and audit server activities.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Finding ID | Vulnerability Name | **Risk Level** | Description | Affected Systems | Machine | Recommendation |
| CVE-2024-0001 | Remote Code Execution (Reverse Shell) | Critical | A remote code execution vulnerability was discovered in the web application, allowing attackers to execute arbitrary code. This can lead to a reverse shell, giving attackers remote control over the affected server. | Web Application (General Functionality) | App1 | Implement stringent input validation, sanitize inputs, and use security measures like WAF and regular patching. Conduct thorough code reviews |
| CVE-2024-0002 | Webmin Remote Code Execution (Reverse Shell) | Critical | Implement stringent input validation, sanitize inputs, and use security measures like WAF and regular patching. Conduct thorough code reviews | Webmin Service (Admin Interface) | SOC 5 | Update Webmin to the latest version, restrict access to trusted IPs, and implement strong authentication mechanisms. Regularly monitor and audit server activities. |

|  |
| --- |
| 1.3 SIGNIFICANT FINDINGS |

## Critical

## Unauthenticated Remote code Execution – RCE



### **Component:**

App1 Server – 192.168.1.121

Status:

Unresolved

### **Description:**

During the security assessment of the App1 server, it was found that an unauthenticated remote code execution vulnerability was present which allows a malicious user to access a broken admin console which allowed access to terminal where an executable was found allowing full root access to the machine.

## Impact:

A malicious actor able to connect to the company intranet can attain full terminal access to the target server to fully compromise the confidentiality, integrity, and availability of the system. Note, since the malicious code is injected directly into memory, this also bypasses anti-virus software.

## Technical fix:

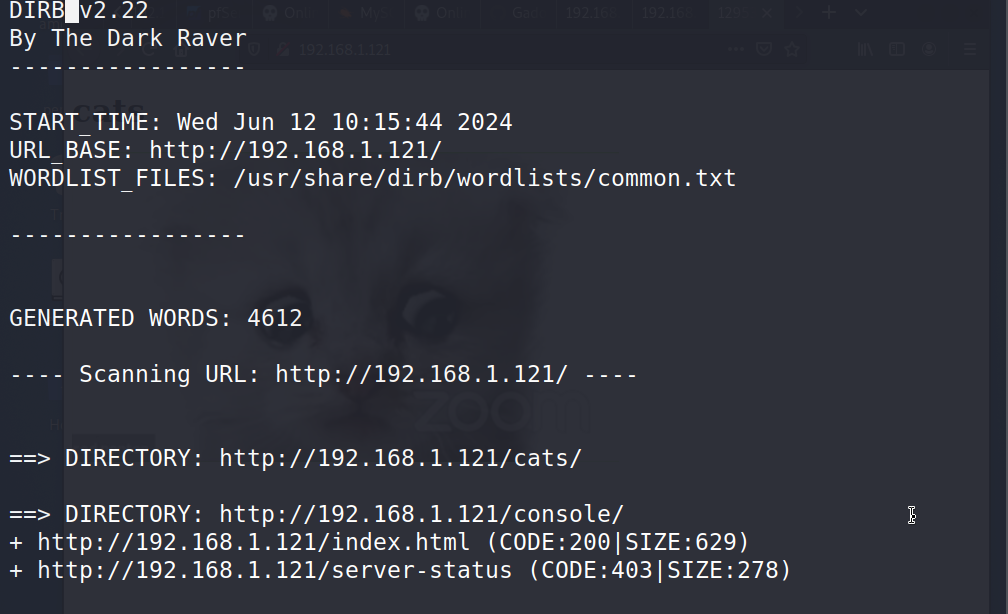
Contact the developer/vendor to request a fix for the admin form so that it does require proper admin credentials and implement input validation to prevent malicious inputs. Also update file permission of the admin executable to only allow users with the correct privileges to run the file.

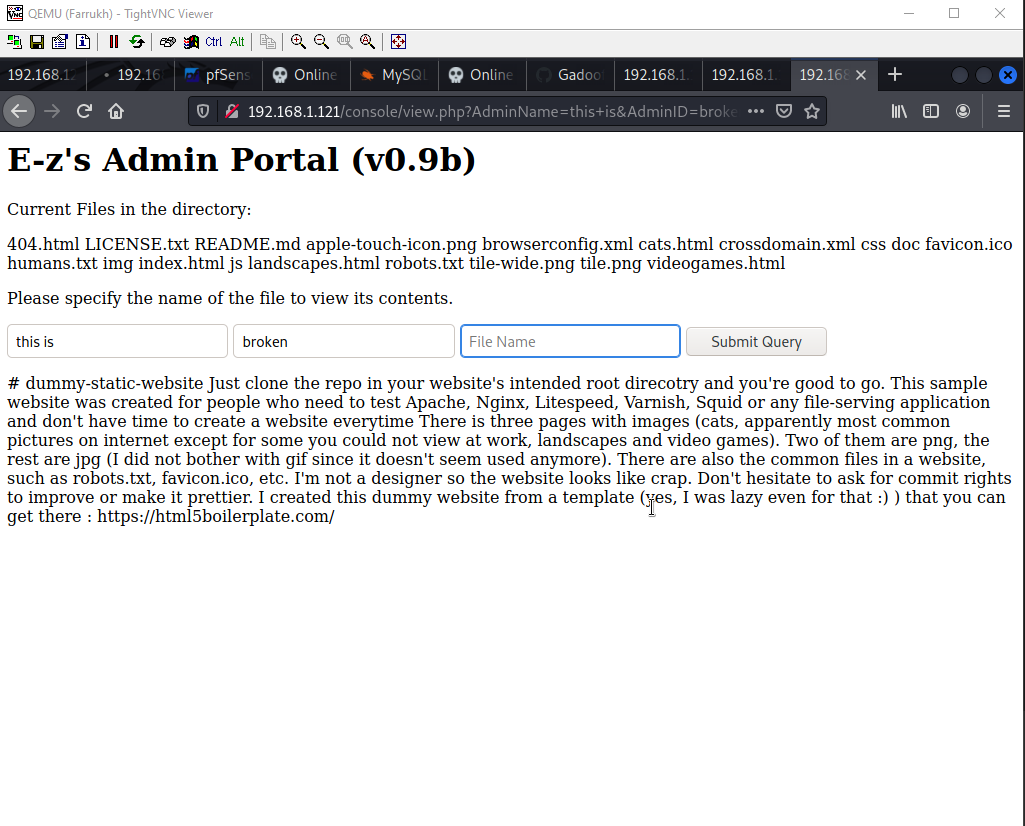
Remediation:

Issue is currently unresolved

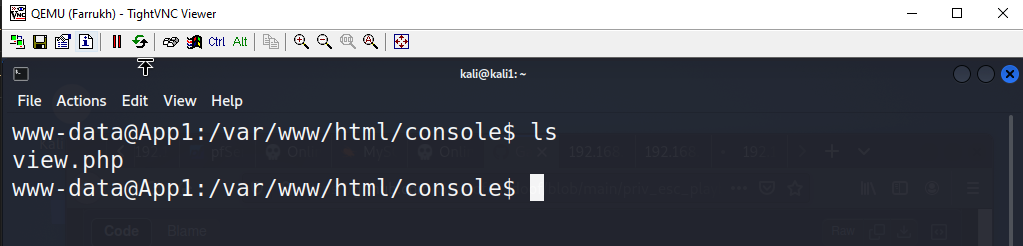
## Technical Details:

It was found that App1 was running a webpage which at first seemed secure but using a directory buster scan found that 2 endpoints were accessible cats and console. The endpoint console had a broken admin form.

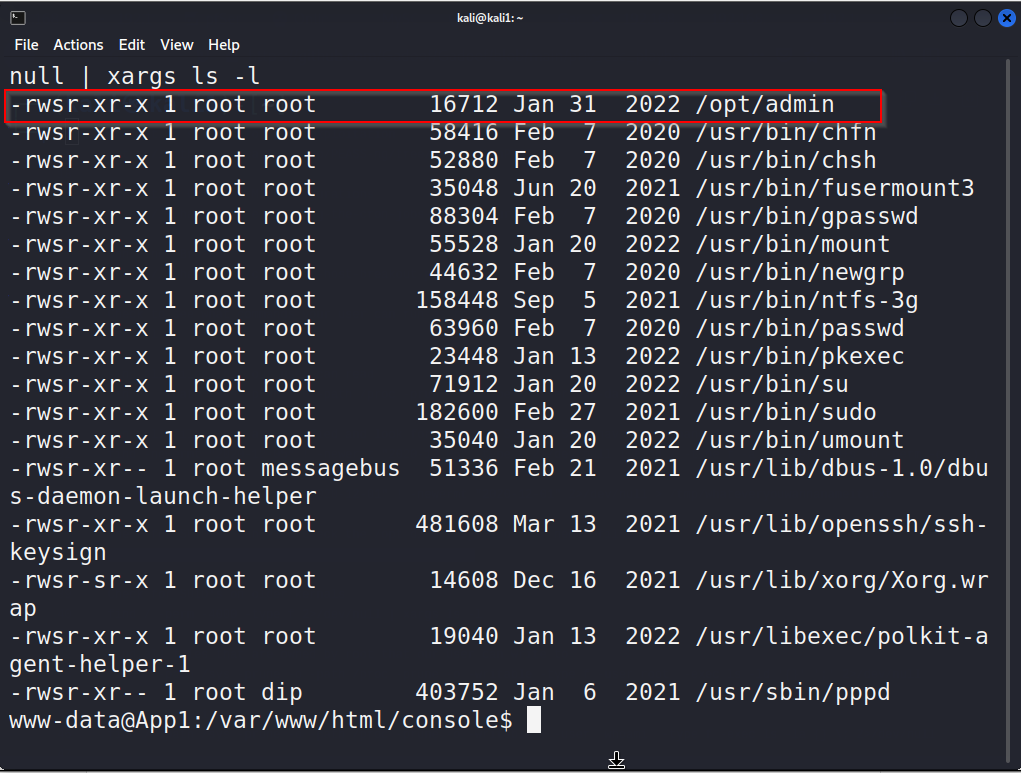




This form was broken and did not have input validation therefore it allowed RCE which allowed us to create a reverse shell. The screenshot below shows the reverse shell fully upgraded and interactable.

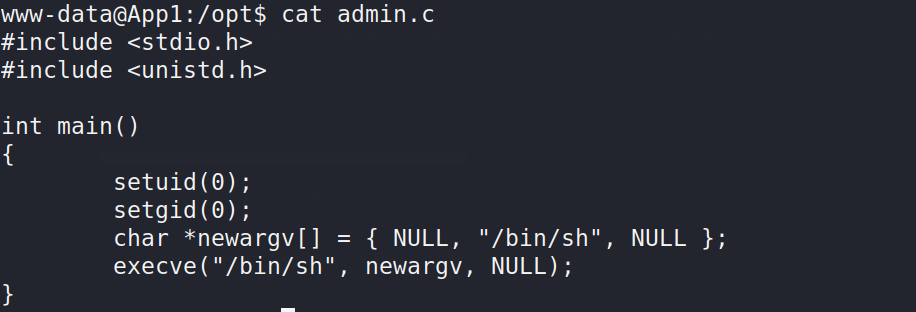


Once we gained access to the system, we searched files on it using the find. We checked for SUIDs using the cmd find / -perm -4000 -type f 2>/dev/null | xargs ls –l this resulted in the response below.



Where we noticed an odd directory not typically found in a Linux system with a file named admin, going to the directory we found compiled code and with the source code.





From the code we found out admin executable turned the user that ran it into admin once ran the file we gained root privileges.



## Critical

## Unauthenticated Remote code Execution – RCE



### **Component:**

SOC 5 – 192.168.1.109

Status:

Unresolved

### **Description:**

During the security assessment of App1, we gained root access, which allowed us to pivot to SOC 5. It was found that an old version of Webmin was installed with a known vulnerability which allowed unauthenticated remote code execution allowing a malicious user to gain root access.

## Impact:

A malicious actor able to connect to the company intranet can obtain full terminal access to the target server to fully compromise the confidentiality, integrity, and availability of the system. Note, since the malicious code is injected directly into memory, this also bypasses anti-virus software.

## Technical fix:

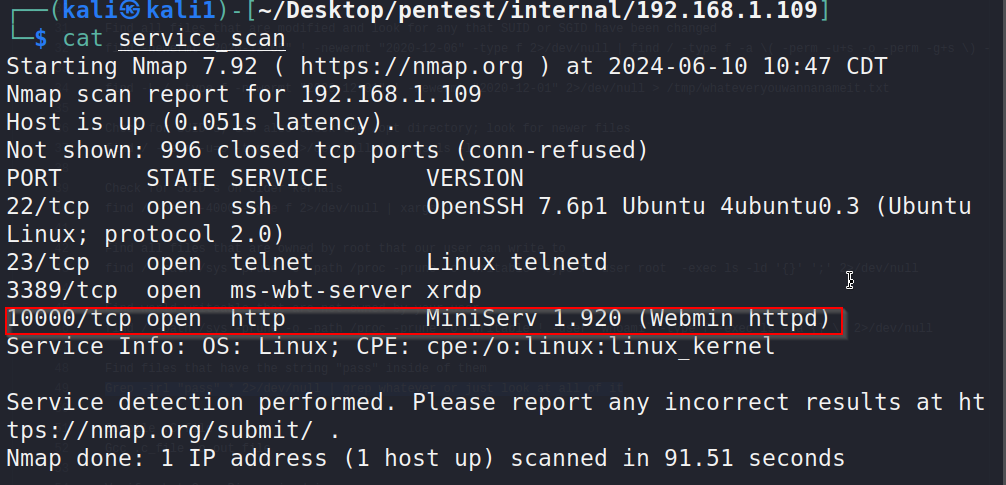
Contact the developer/vendor to update Webmin to the latest version, and implement a policy where applications are reviewed periodically and updated. Also implement a security control to only allow secured Ip addresses to access the server.

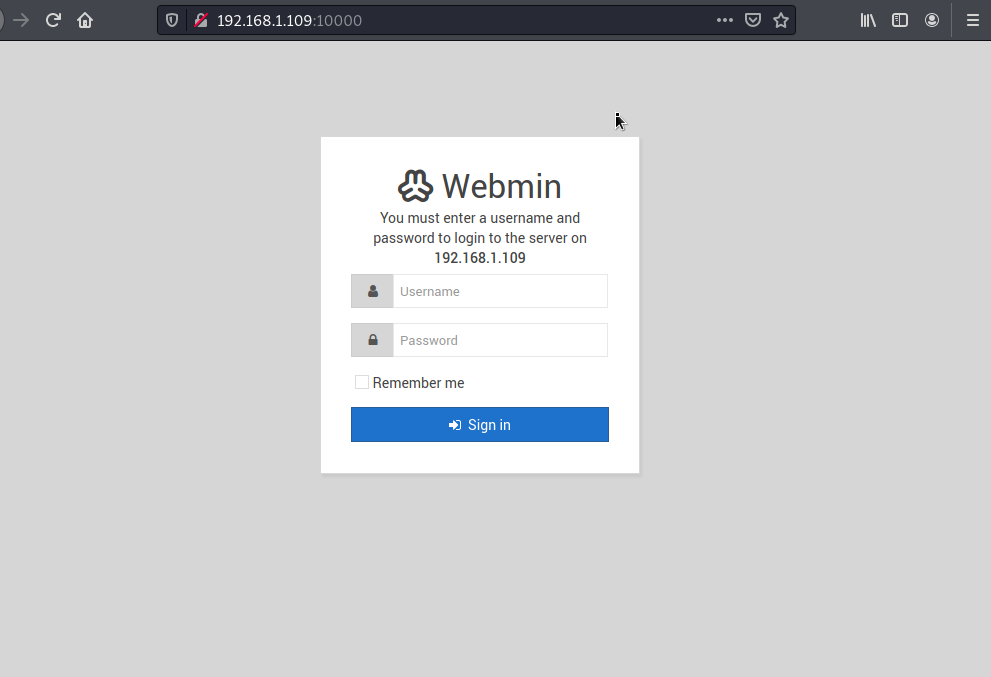
Remediation:

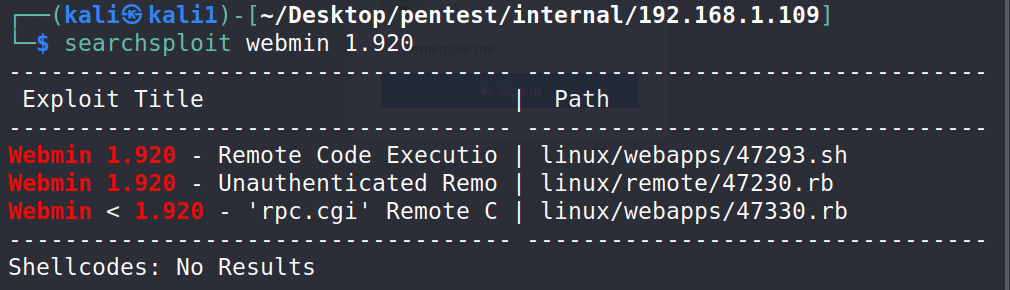
Issue is currently unresolved

## Technical Details:

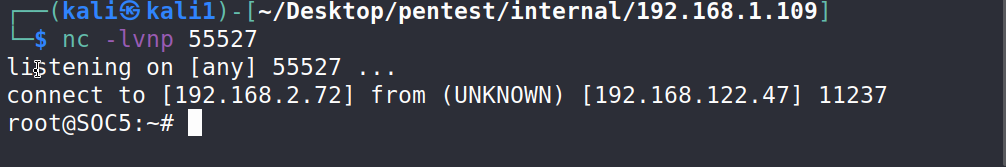
Continuing from previous root privileges gained from App1, a Nmap scan was done to pivot from to other devices. From the scan it was found that SOC 5 had multiple ports open



Researching port 10000 resulted in the following webpage where an outdated version of Webmin with known vulnerability deployed



Once a reverse shell was created with Metasploit a proxy was then created to created persistent connection allowing further pen testing of the network



# Flags

## SOC 5

### **Flag 1**

Details: A file named root.txt was found in the root directory.

Flag Content: ‘SOC5: TECHSUPPORT: 30 POINTS’

### **Flag 2**

Details: A file named flag.txt was found in the home directory.

Flag Content: SOC5: GNS3: 15 POINTS

