Grace Testerman

V1.2

February 4, 2025

Penetration Assessment



# **Document Properties**

|  |  |
| --- | --- |
| **Title** | Penetration Assessment of De-Ice virtual machines |
| **Author** | Grace Testerman |

## **Versioning Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Changes** |
| V1.0 | December 17th, 2023 | Grace Testerman | Created the document |
| V1.2 | February 4th, 2025 | Grace Testerman | Modified the document |

**Disclaimer:** This document and its findings is a purely fictitious penetration testing report for the purpose of learning and training. All reconnaissance, password cracking, and exploiting was done in a sandbox environment consisting of virtual machines and does not represent any actual networks or systems of any organization.

# **Executive Summary**

This document reports on the penetration assessment of four virtual machines: De-Ice S1.100, De-Ice S1.110, De-Ice S1.120, and De-Ice S1.140. The purpose of this assessment is to identify vulnerabilities and gain access to sensitive information hosted on these machines. Additionally, this assessment will identify which fundamental security design principles are in play, how they interrelate, and methods in which they should be applied to develop systems worthy of trust.

**Table of Contents**

[**Document Properties** 1](#_Toc153746687)

[**Versioning Control** 1](#_Toc153746688)

[**Executive Summary** 1](#_Toc153746689)

[**1.** **De-Ice S1.100** 3](#_Toc153746690)

[**Summary** 3](#_Toc153746691)

[**Recommendations** 3](#_Toc153746692)

[**Scope** 3](#_Toc153746693)

[**Details** 3](#_Toc153746694)

[**Recon** 3](#_Toc153746695)

[**Scanning** 3](#_Toc153746696)

[**Exploit** 3](#_Toc153746697)

[**Report** 4](#_Toc153746698)

[**2.** **De-Ice S1.110** 4](#_Toc153746699)

[**Summary** 4](#_Toc153746700)

[**Recommendations** 4](#_Toc153746701)

[**Scope** 4](#_Toc153746702)

[**Details** 5](#_Toc153746703)

[**Recon** 5](#_Toc153746704)

[**Scanning** 5](#_Toc153746705)

[**Exploit** 5](#_Toc153746706)

[**Report** 5](#_Toc153746707)

[**3.** **De-Ice S1.120** 6](#_Toc153746708)

[**Summary** 6](#_Toc153746709)

[**Recommendations** 6](#_Toc153746710)

[**Scope** 6](#_Toc153746711)

[**Details** 6](#_Toc153746712)

[**Recon** 6](#_Toc153746713)

[**Scanning** 7](#_Toc153746714)

[**Exploit** 7](#_Toc153746715)

[**Report** 7](#_Toc153746716)

[**4.** **De-Ice S1.140** 8](#_Toc153746717)

[**Summary** 8](#_Toc153746718)

[**Recommendations** 8](#_Toc153746719)

[**Scope** 8](#_Toc153746720)

[**Details** 8](#_Toc153746721)

[**Recon** 8](#_Toc153746722)

[**Scanning** 8](#_Toc153746723)

[**Exploit** 8](#_Toc153746724)

[**Report** 10](#_Toc153746725)

# **De-Ice S1.100**

## **Summary**

This assessment utilizes a Kali Linux virtual machine to perform a penetration test on the De-Ice S1.100 machine (192.168.1.100). This was done to discover the vulnerabilities of the machine and attempt to gain access to the root user account. A more detailed analysis of this test can be found in the “Details” section of this report.

## **Recommendations**

Alert the company of all outstanding vulnerabilities.

## **Scope**

A Kali Linux virtual machine was used in a sandbox environment to attempt to gain root access to the vulnerable De-Ice S1.100 machine (192.168.1.100).

## **Details**

### **Recon**

Passive reconnaissance of the De-Ice S1.100 machine was performed by using the Firefox browser to view the penetration testing lab. From there, information was found about the names and emails for various departments of the organization, including the financial and engineering departments. At the bottom of the page, the names and emails of the three system administrators were given.

### **Scanning**

The Kali Linux machine was able to scan the target (192.168.1.100) using Nmap. From there, it was discovered that the machine had open ftp, ssh, smtp, http, pop3, and imap ports. Additionally, the operating system for the server appeared to be Unix.

### **Exploit**

Metasploit was utilized in the Kali Linux VM to exploit possible usernames and passwords for the target machine through the open ssh port. This was done through the exploit ***scanner/ssh/ssh\_login*** on a text document containing possible usernames for the system administrators. After running the exploit, it was discovered that there was a user account containing the username and password “bbanter”. This allowed bbanter’s account to be logged into through the ssh port. Using this account, it was possible to find the usernames for the other system administrators. The Metasploit exploit was then used again to find the password for aadams’s account. Using the aadams account, it was possible to find the password hashes for all user accounts in the target system’s directory, including the root account. After placing the root password hash into a text file, the John the Ripper tool was used to discover the root password.

### **Report**

Through logging into aadam’s account in the ssh port, the root password was utilized to gain access to the root account. For more information, see the documented screenshot below.

A screenshot of a computer screen

Description automatically generated

# **De-Ice S1.110**

## **Summary**

This assessment utilizes a Kali Linux virtual machine to perform a penetration test on the De-Ice S1.110 machine (192.168.1.110). This was done to discover the vulnerabilities of the machine and attempt to gain access to the root user account. A more detailed analysis of this test can be found in the “Details” section of this report.

## **Recommendations**

Alert the company of all outstanding vulnerabilities.

## **Scope**

A Kali Linux virtual machine was used in a sandbox environment to attempt to gain root access to the vulnerable De-Ice S1.110 machine (192.168.1.110). Tools utilized in this assessment include Nmap and John the Ripper.

## **Details**

### **Recon**

Reconnaissance was performed on the target machine through the Firefox browser in the Kali Linux VM. While looking at the html index of the machine, the names and emails of the system admins were discovered. These names and emails include:

Sr. System Admin: Adam Adams – adamsa@herot.net

System Admin (Intern): Bob Banter – banterb@herot.net

System Admin: Chad Coffee – coffeec@herot.net

### **Scanning**

In addition to passive reconnaissance, scanning was performed on the machine through the use of Nmap. This was done through the following command:

**nmap -sV -O 192.168.1.110**

The scan report found several open ports on the target, including ftp, tcpwrapped, http, and ipp. Additionally, the report discovered that the machine was running on a Unix operating system.

### **Exploit**

The target’s vulnerable ftp port was connected through the Kali Linux machine through an anonymous account. From there, the file system could be accessed, and the “shadow” file was found to contain password hashes. These hashes were cracked using John the Ripper to find the following passwords:

Root – Complexity

Ccoffee – Diatomaceous

Bbanter – Zymurgy

### **Report**

The root password did not work when logging into ssh; however, bbanter’s password did work. From the connected ssh terminal, the command “su” was used to get sudo privileges, and when prompted, the “Complexity” password worked. When using the “whoami” command, root status was displayed. For more detailed information, see the documented screenshot below.

A computer screen shot of a computer program

Description automatically generated

# **De-Ice S1.120**

## **Summary**

This assessment utilizes a Kali Linux virtual machine to perform a penetration test on the De-Ice S1.120 machine (192.168.1.120). This was done to discover the vulnerabilities of the machine and attempt to gain access to the root user account. A more detailed analysis of this test can be found in the “Details” section of this report.

## **Recommendations**

Alert the company of all outstanding vulnerabilities, including the public data entry site and open mysql port.

## **Scope**

A Kali Linux virtual machine was used in a sandbox environment to attempt to gain root access to the vulnerable De-Ice S1.120 machine (192.168.1.120). Tools used in this assessment include Nmap and SQLMap.

## **Details**

### **Recon**

Recon was performed on the target machine by viewing the server (192.168.1.120) on the Kali Linux VM’s Firefox browser. When connecting to the machine on the browser, a data entry site was found. It appears that this site was not meant to be publicly accessible, and the IT staff was not interested in maintaining the site.

### **Scanning**

After initial reconnaissance, scanning was performed on the target machine (192.168.1.120) through the use of Nmap. To do this, the following command was performed:

**nmap -sV -O 192.168.1.120**

When analyzing the scan report, it was discovered that the machine had several open ports, including ftp, ssh, http, ssl/http, and mysql. Additionally, it was found that the machine was running on a Linux operating system.

### **Exploit**

The open mysql port was exploited through the use of SQLMap in Kali Linux to crack passwords on the target machine. To do this, the following commands were used.

**sqlmap -u 192.168.1.120/products.php?id=1 -dbs -batch**

**sqlmap -u 192.168.1.120/products.php?id=1 -D mysql –tables**

**sqlmap -u 192.168.1.120/products.php?id=1 -D mysql -users -passwords**

It was then discovered that the user ccoffee’s password was “batman”. The account was successfully logged into the machine remotely through ssh.

### **Report**

After successfully connecting to the ccoffee account through ssh, the script “getlogs.sh” was discovered. This script was modified and ran with sudo privileges to gain root access. For more information, see the screenshot documented below.

**A computer screen with green text

Description automatically generated**

# **De-Ice S1.140**

## **Summary**

This assessment utilizes a Kali Linux virtual machine to perform a penetration test on the De-Ice S1.140 machine (192.168.1.140). This was done to discover the vulnerabilities of the machine and attempt to gain access to the root user account. A more detailed analysis of this test can be found in the “Details” section of this report.

## **Recommendations**

Alert the company of all outstanding vulnerabilities.

## **Scope**

A Kali Linux virtual machine was used in a sandbox environment to attempt to gain root access to the vulnerable De-Ice S1.140 machine (192.168.1.140). Tools used in this assessment include Nmap, DIRB, Jack the Ripper, and OpenSSL.

## **Details**

### **Recon**

When first looking at the machine through the Firefox browser, not much is shown. The only information that is seen includes hints about how to get the sensitive information in the Lab.

### **Scanning**

Nmap was utilized to scan the target machine. Upon analyzing the scan report, it was discovered that several ports were open, including ftp, ssh, http, ssl/http, ssl/imap, and ssl/pop3. Additionally, the machine appeared to be running on a Unix operating system.

After the Nmap scan, additional scanning was made through the use of DIRB. This scan was made to look for additional web content from the target and resulted with the interesting /forum directory (https://192.168.1.140/forum/). Upon further reconnaissance of the forum, a post titled “Login Attacks” was found with authentication logs trying hundreds of different logins into the system.

### **Exploit**

The authentication logs were exploited to find the password of one of the system user accounts. This was done through the following commands:

**cat file.txt | grep “Invalid user” | awk ‘{print $8}’**

**cat file.txt | grep “open”**

The results found one opened session with mbrown’s account and the password **“!DFiuoTkbxtdk0!”. These credentials were utilized to log into mbrown’s account in the forum directory and find his email (mb@lazyadmin.corp). This email was logged into using the same password in the webmail directory (https://192.168.1.140/webmail/src/login.php). Found inside the mailbox was the following mysql login information:**

**Username: root**

**Password:** S4!y.dk)j/\_d1pKtX1

These root credentials were able to be successfully authenticated into the phpMyAdmin directory of the target (https://192.168.1.140/phpmyadmin/). From there, the usernames, password hashes, and names of four accounts were discovered: Richard Hedley, Sandy Willard, Mark Brown, and Miles Parker. From a simple md5 decription, two of the four passwords were discovered.

rhedley: tum-ti-tum

swillard: Austin-Willard

The other two hashes were unable to be decrypted.

After these credentials were found, rhedley’s account was able to be connected with FTP through the following command:

**ftp 192.168.1.140**

With this connection, the backup file ***backup\_webhost\_130111.tar.gz.enc*** was downloaded through the following command:

**get backup\_webhost\_130111.tar.gz.enc**

Additionally, there was a .ssh directory where the key “downloadkey” could be downloaded for mbrown. This was downloaded through the “**get download**” command.

After these downloads were made and the private key was edited for ssh, a successful connection could be made to the ssh port through mbrown’s account. Once this was completed, the following commands were made:

**su rhedley**

**cd /opt**

**ls**

**cat bakup.sh**

These commands were used to find and download a file containing the password for the backup file. It was then decrypted through the following command:

**openssl aes-256-cbc -d -md md5 -in backup\_webhost\_130111.tar.gz.enc -out file.tar.gz -pass pass:wpaR9V616xrDTy98L7Uje2DDU5hWtWhs**

**tar -xvf file.tar.gz**

These commands gave a shadow file which can be opened with the next two commands:

**cd etc**

**cat shadow**

from there, the password hashes for three users can be analyzed. To crack these hashes, John the Ripper was used to find the final credentials necessary to gain root access:

User: sraines

Password: brillantissimo

### **Report**

To get to root, mbrown can be used again to log into ssh with the following command:

**ssh -i downloadkey mbrown@192.168.1.140**

From there, the user can be switched to swillard:

**su swillard**

Upon viewing the /forums directory, it can be seen that sraines changed her username to swillard. We can log into swillard’s account with the “brillantissimo” password. After successfully logging in, we can reach the root directory through the following commands:

**sudo -l**

**sudo su**

**cd /root**

**whoami**

For more information about this assessment, see the screenshot documented below.

A computer screen with green text

Description automatically generated