# Password Auditor - Find Weak Credentials Report

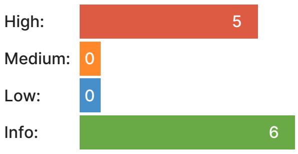
✓ **mail.pentest-ground.com**

## Summary

**Overall risk level:**

High

**Risk ratings:**



**Scan information:**

| | |
|---|---|
| Start time: | 2023-01-20 18:02:50 UTC+02 |
| Finish time: | 2023-01-20 18:15:55 UTC+02 |
| Scan duration: | 13 min, 5 sec |
| Tests performed: | 11/11 |
| Scan status: | Finished |

## Findings

### HTTPS Weak Password (port 443)

| Server | Open Port | Service | Username | Password | URL |
|---|---|---|---|---|---|
| mail.pentest-ground.com | 443 | https | administrator | soccer | https://mail.pentest-ground.com/owa/auth/logon.aspx?url=https%3a%2f%2fmail.pentest-ground.com%2fowa%2f&reason=0 |

Details

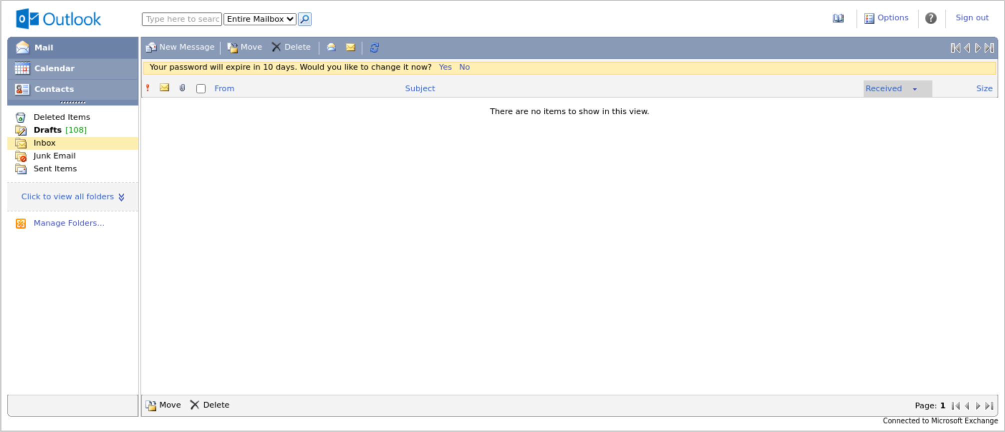
**Vulnerability description:**
The service is vulnerable to brute-force attacks because a weak password is configured.

**Risk description:**
The risk exists that a remote unauthenticated attacker can login through the service and compromise the server in order to steal sensitive information, install ransomware or pivot to the internal network.

**Recommendation:**
We recommend always changing the default passwords to more secure and uncommon ones, that should be at least 8 characters long and contain a mixture of lowercase, uppercase letters, numbers and special characters.
You may also enforce a maximum number of incorrect attempts (3, for example) when someone tries to authenticate, before blocking the system for a period of time.

**References:**
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy

**Screenshot:**



Your password will expire in 10 days. Would you like to change it now? Yes No

There are no items to show in this view.

Connected to Microsoft Exchange

Figure 1.

## SMB Weak Password (port 445)

| Server | Open Port | Service | Username | Password |
|---|---|---|---|---|
| mail.pentest-ground.com | 445 | microsoft-ds | administrator | soccer |

Details

**Vulnerability description:**
The service is vulnerable to brute-force attacks because a weak password is configured.

**Risk description:**
The risk exists that a remote unauthenticated attacker can login through the service and compromise the server in order to steal sensitive information, install ransomware or pivot to the internal network.

**Recommendation:**
We recommend always changing the default passwords to more secure and uncommon ones, that should be at least 8 characters long and contain a mixture of lowercase, uppercase letters, numbers and special characters.
You may also enforce a maximum number of incorrect attempts (3, for example) when someone tries to authenticate, before blocking the system for a period of time.

**References:**
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy

## MSSQL Default Credentials Found (port 1433)

| Server | Open Port | Service | Username | Password |
|---|---|---|---|---|
| mail.pentest-ground.com | 1433 | ms-sql-s | sa | [blank] |

Details

**Vulnerability description:**
The service has default or commonly known credentials configured.

**Risk description:**
The risk exists that a remote unauthenticated attacker can login through the service and compromise the server in order to steal sensitive information, install ransomware or pivot to the internal network.

**Recommendation:**
We recommend always changing the default passwords to more secure and uncommon ones, that should be at least 8 characters long and contain a mixture of lowercase, uppercase letters, numbers and special characters.
You may also enforce a maximum number of incorrect attempts (3, for example) when someone tries to authenticate, before blocking the system for a period of time.

**References:**

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy

## 🟥 RDP Weak Password (port 3389)

| Server | Open Port | Service | Username | Password |
|---|---|---|---|---|
| mail.pentest-ground.com | 3389 | ms-wbt-server | administrator | soccer |

Details

**Vulnerability description:**
The service is vulnerable to brute-force attacks because a weak password is configured.

**Risk description:**
The risk exists that a remote unauthenticated attacker can login through the service and compromise the server in order to steal sensitive information, install ransomware or pivot to the internal network.

**Recommendation:**
We recommend always changing the default passwords to more secure and uncommon ones, that should be at least 8 characters long and contain a mixture of lowercase, uppercase letters, numbers and special characters.
You may also enforce a maximum number of incorrect attempts (3, for example) when someone tries to authenticate, before blocking the system for a period of time.

**References:**
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy

## 🟥 WinRM Weak Password (port 5985)

| Server | Open Port | Service | Username | Password |
|---|---|---|---|---|
| mail.pentest-ground.com | 5985 | wsman | administrator | soccer |

Details

**Vulnerability description:**
The service is vulnerable to brute-force attacks because a weak password is configured.

**Risk description:**
The risk exists that a remote unauthenticated attacker can login through the service and compromise the server in order to steal sensitive information, install ransomware or pivot to the internal network.

**Recommendation:**
We recommend always changing the default passwords to more secure and uncommon ones, that should be at least 8 characters long and contain a mixture of lowercase, uppercase letters, numbers and special characters.
You may also enforce a maximum number of incorrect attempts (3, for example) when someone tries to authenticate, before blocking the system for a period of time.

**References:**
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy

## 🟩 Found 9 open ports

| Server | Open Port | Service | URL |
|---|---|---|---|
| mail.pentest-ground.com | 80 | http | http://mail.pentest-ground.com:80/ |

| | | | |
|---|---|---|---|
| mail.pentest-ground.com | 81 | http | http://mail.pentest-ground.com:81/ |
| mail.pentest-ground.com | 443 | https | https://mail.pentest-ground.com/owa/auth/logon.aspx?url=https%3a%2f%2fmail.pentest-ground.com%2fowa%2f&reason=0 |
| mail.pentest-ground.com | 444 | https | https://mail.pentest-ground.com:444/ |
| mail.pentest-ground.com | 445 | microsoft-ds | - |
| mail.pentest-ground.com | 1433 | ms-sql-s | - |
| mail.pentest-ground.com | 3389 | ms-wbt-server | - |
| mail.pentest-ground.com | 5985 | wsman | - |
| mail.pentest-ground.com | 6001 | http | http://mail.pentest-ground.com:6001 |

Details

**Risk description:**
This is the list of ports that have been found open on the target host.
Having unnecessary open ports may expose the target system to risks because those network services and applications may contain vulnerabilities.

**Recommendation:**
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

## Could not attempt authentication on service HTTP (port 80)

## Could not attempt authentication on service HTTP (port 81)

## Could not attempt authentication on service HTTPS (port 444)

## No MSSQL Weak Password Found (port 1433)

## Could not attempt authentication on service HTTP (port 6001)

## Scan coverage information

### List of tests performed (11/11)

- ✓ Scanning target for open ports...
- ✓ Checking service connectivity on port 80...
- ✓ Checking service connectivity on port 81...
- ✓ Searching for weak credentials on port 443...
- ✓ Checking service connectivity on port 444...
- ✓ Searching for weak credentials on port 445...
- ✓ Searching for default credentials on port 1433...
- ✓ Searching for weak credentials on port 1433...

- ✓ Searching for weak credentials on port 3389...
- ✓ Searching for weak credentials on port 5985...
- ✓ Checking service connectivity on port 6001...

### Scan parameters

| | |
|---|---|
| Target: | mail.pentest-ground.com |
| Attack type: | dictionary |
| Ports: | Top 100 ports |
| Services: | AMQP, Docker, FTP, HTTP, MQTT, MSSQL, MySQL, PostgreSQL, RDP, Redis, SMB, SSH, STOMP, Telnet, VNC, WinRM |
| Usernames: | default |
| Passwords: | default |
| Time delay between attempts: | none |
| Lockout period: | none |
| Attempts per period: | none |
| Check default credentials: | True |