Password Auditor - Find Weak Credentials Report

✔ **mail.pentest-ground.com**

Summary

Overall risk level:

High

Risk ratings:

High:	4
Medium:	0
Low:	0
Info:	1

Scan information:

Start time:	Apr 29, 2024 / 15:36:59
Finish time:	Apr 29, 2024 / 15:37:38
Scan duration:	39 sec
Tests performed:	5/5
Scan status:	Finished

Findings

HTTPS Weak Password

port 443

Server	Open Port	Service	Username	Password	URL
mail.pentest-ground.com	443	https	Administrator	P@ssw0rd2024	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:

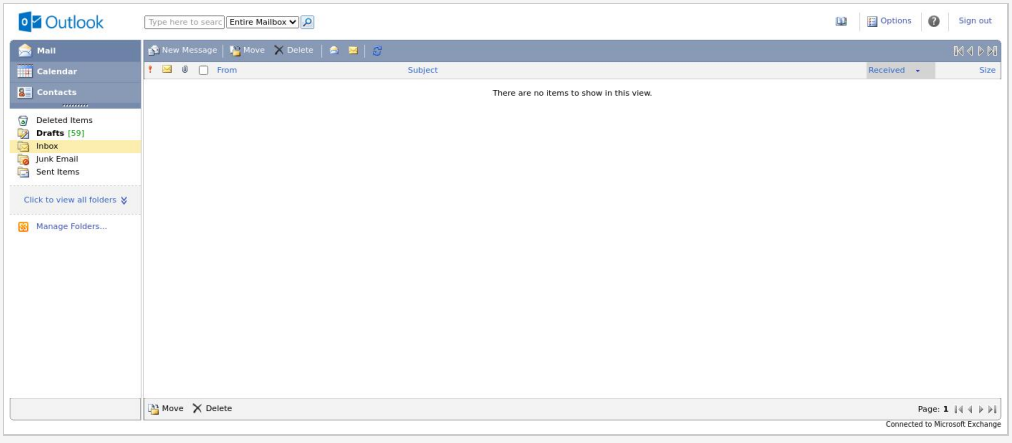

Figure 1.

SMB Weak Password

port 445

Server	Open Port	Service	Username	Password
mail.pentest-ground.com	445	microsoft-ds	Administrator	P@ssw0rd2024

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

RDP Weak Password

port 3389

Server	Open Port	Service	Username	Password
mail.pentest-ground.com	3389	ms-wbt-server	Administrator	P@ssw0rd2024

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	P@ssw0rd2024

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 4 open ports

Server	Open Port	Service	URL
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	445	microsoft-ds	-
mail.pentest-ground.com	3389	ms-wbt-server	-
mail.pentest-ground.com	5985	wsman	-

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.

Scan coverage information

List of tests performed (5/5)

- Scanning target for open ports...
- Searching for weak credentials on port 443...
- Searching for weak credentials on port 445...
- Searching for weak credentials on port 3389...
- Searching for weak credentials on port 5985...

Scan parameters

Target:	mail.pentest-ground.com
Attack type:	dictionary
Ports:	443,445,1433,3389,5985
Services:	AMQP, Docker, FTP, HTTP, MQTT, MSSQL, MySQL, PostgreSQL, RDP, Redis, SMB, SSH, STOMP, Telnet, VNC, WinRM
Usernames:	Test Wordlist (1 words)
Passwords:	Test passwords wordlist (custom) (1 words)
Time delay between attempts:	0s
Lockout period:	none
Attempts per period:	none
Check default credentials:	False