| Document Name | Testing Report – Brute-Force Protection on Windows Server 2022 (Playbook 1) | Version | 1.0 |
|---|---|---|---|
| Author | Anusha Ramu Chakravarthi | Date Created | 24/04/2025 |
| Test Type | Brute-Force Protection Testing (RDP and SMB) | Last Modified | 12/05/2025 |

## Purpose

This report summarizes the results from testing the brute-force protection mechanisms implemented on Windows Server 2022. It evaluates the effectiveness of **RDP Guard** for RDP, and **Windows Firewall + Account Lockout Policies** for SMB, against known attack tools.

## Tools Used

- **Hydra**: Used for RDP brute-force testing.
- **CrackMapExec (CME)**: Used for SMB brute-force testing.
- **Metasploit**: Used for SMB brute-force testing.

## Test Procedures

1. **RDP Brute-Force Testing**
    - Tool: **Hydra**
    - Target: **Windows Server 2022 RDP**
    - Protection: **RDP Guard**
    - Test Setup: Attack initiated from Kali VM using Hydra to simulate multiple RDP login attempts.

2. **SMB Brute-Force Testing**
    - Tool: **CrackMapExec (CME)**
    - Target: **SMB (port 445) on Windows Server 2022**
    - Protection: **Account Lockout Policy, Windows Firewall**
    - Test Setup: Attack simulated using CME to enumerate valid usernames and attempt login.

3. **SMB Brute-Force Testing with Metasploit**
    - Tool: **Metasploit (auxiliary/scanner/smb/smb_login)**
    - Target: **Windows Server 2022 SMB**
    - Protection: **Account Lockout Policy, Windows Firewall, SMB Hardening**
    - Test Setup: Attack simulated using Metasploit's SMB login scanner module.

## Observations

- **RDP Brute-Force Testing with Hydra**
  - **Testing Outcome**:
    - Hydra successfully attempted RDP brute-force.
    - **RDP Guard** detected repeated failed attempts and blocked the Kali VM's IP after exceeding the configured threshold (e.g., 3 attempts).
    - Once blocked, further Hydra attempts failed to establish a connection (freerdp: the connection failed to establish).
    - **Event ID 4625** (failed logons) was logged.
    - **Event ID 4740** (account lockout) did not always appear unless auditing was correctly configured on the domain controller.
  - **Conclusion**:
    - **RDP Guard** effectively blocks IPs performing brute-force attacks.
    - **Account lockout policy** must be reviewed and verified for Event ID 4740 logging.

- **SMB Brute-Force Testing with CrackMapExec (CME)**
  - **Testing Outcome**:
    - **CME** was able to enumerate valid usernames based on SMB error responses.
    - Even after the account was locked out, **CME** sometimes showed valid creds due to how SMB responds before full authentication.
    - Account lockout was eventually triggered, but valid credentials were still highlighted.
    - **Event ID 4740** may not always log unless lockout auditing is correctly configured in the Default Domain Controller Policy.
  - **Conclusion**:
    - **SMB brute-force protection** partially works: accounts get locked out, but tools like CME can still enumerate valid usernames and credentials due to **SMB protocol limitations**.
    - **Additional protection** may require **IDS/IPS** or third-party endpoint protection.

- **SMB Brute-Force Testing with Metasploit**
  - **Testing Outcome**:
    - **Metasploit** successfully enumerated valid credentials (green plus) despite the account lockout policy.
    - Account lockout occurred only after multiple attempts—valid users were identified before lockout was triggered.
    - **Event ID 4625** (failed logons) was consistently logged.
    - **Event ID 4740** (account lockout) only appeared when auditing was explicitly enabled on the Default Domain Controller Policy.
    - **Firewall filtering** (block SMB from Kali) was effective in preventing further brute-force attacks once activated.
  - **Observation**:
    - **Metasploit's scanner module** is highly threaded and aggressive, which can discover valid credentials before lockout enforcement kicks in. This highlights a limitation in **Windows lockout policy** effectiveness against fast, parallel brute-force tools.
  - **Mitigations Explored**:
    - **Stricter firewall rules** to limit external SMB access.
    - Exploring **network-level protections** using pfSense IDS/IPS (e.g., **Suricata/Snort**).
    - Considering **PowerShell-based alerting scripts** to disable accounts or alert admins after X failed logons.

## Conclusion

- **RDP Guard** provides effective protection against brute-force attacks by blocking IPs after repeated failed login attempts.
- **SMB brute-force protection** works to some extent but can be bypassed by tools like **CME** and **Metasploit**, which can still enumerate valid usernames before lockout occurs. **Additional protections**, such as **IDS/IPS** or third-party endpoint solutions, may be needed.
- **Account lockout policies** should be carefully reviewed to ensure that event logging is correctly configured for audit purposes.

## Recommendations

1. **For RDP**:
    - Consider enabling **Geo-IP filtering** or implementing **Two-Factor Authentication (2FA)** to further harden RDP access.
2. **For SMB**:
    - Consider segmenting **SMB access** and restricting services via **Group Policy Objects (GPO)**.
    - Implement **advanced threat detection tools** (e.g., **IDS/IPS** like Suricata/Snort) to catch aggressive brute-force tools.
    - Use **PowerShell-based scripts** to disable accounts or alert administrators after a set number of failed logins.