Bug Report Documentation

Bug Title:

ARPSpoof Module Fails to Execute :Process Terminated with Exit Code 1

Bug Type:

- Functional Bug
- Configuration Bug
- Usability Bug

Severity: HIGH

The failure prevents the execution of the ARP spoofing module, directly impacting the core functionality of the cybersecurity testing tool.

Environment:

- Virtual Machine (VirtualBox)
- Cybersecurity Testing Toolkit
- Network-based attack module (ARPSpoof)

Description:

During testing of the ARPSpoof module, the tool failed to execute and displayed the error message:

“Process terminated with exit code: 1.”

This indicates that the command stopped unexpectedly due to missing requirements or incorrect configuration. As a result, the attack simulation could not proceed.

Such failures reduce tool reliability and may confuse users who are attempting to perform legitimate security testing.

Steps to Reproduce:

1. Launch the cybersecurity toolkit inside the virtual machine.
2. Navigate to the ARPSpoof configuration page.
3. Enter target IP addresses.
4. Start the spoofing process.
5. Observe the system output.

Actual Result:

The system terminates the process immediately and displays:

Exit code: 1

No clear explanation or remediation guidance is provided to the user.

Expected Result:

The system should:

- Validate prerequisites before execution.
- Provide a clear error message explaining the failure.
- Suggest corrective actions.
- Prevent execution until configuration requirements are met.

The failure is most likely caused by one or more of the following configuration issues:

1. Insufficient Privileges

ARP spoofing requires superuser permissions because it interacts directly with network interfaces.

Impact:
Without root access, the command cannot modify ARP tables and will terminate.

Recommendation:
Implement a privilege check before execution and notify users to run the tool with administrative rights.

2. Missing or Incorrect Network Interface

The ARPSpoof command requires a valid interface parameter.

If the interface is not selected or detected automatically, execution fails.

Recommendation:
Provide an interface selection dropdown and enforce it as a mandatory field.

3. Invalid Target Network

If the provided IP addresses are not within the same subnet as the testing machine, the tool cannot communicate with the targets.

Recommendation:

- Validate IP subnet compatibility.
- Perform a reachability test before launching the attack.

4. Virtual Machine Network Misconfiguration

When the VM is configured in **NAT mode**, ARP spoofing attacks typically fail because NAT isolates network traffic.

Recommendation:
Notify users to use:

Bridged Adapter
or

Host-only network

for controlled lab environments.

Security Impact

Although this is primarily a functional failure, it has security implications:

- Prevents accurate penetration testing
- Reduces trust in tool outputs
- May lead to incorrect security assessments
- Impacts learning outcomes in lab environments

Reliable tools are essential for effective vulnerability analysis.

Usability Impact

The error message lacks clarity and does not assist the user in troubleshooting.

Observed Issues:

- No explanation of the failure
- No suggested fix
- Technical output without context

Recommendation:
Replace generic exit codes with actionable messages such as:

Execution failed: Root privileges required.
“Execution failed: No network interface selected.”

Ethical Consideration

ARP spoofing tools must only be used in:

- Authorized cybersecurity labs
- Approved penetration testing scenarios

Unauthorized use may violate legal and ethical standards.