Phase 4: Threat Assessment

Goal:
Create a hypothetical threat assessment based on vulnerabilities you expect to find when you perform your actual scans against the client's network.

Procedure:
Assume the scenarios below are what you most likely will encounter when the testing begins.

Deliverable:
Provide a spreadsheet or document showing the following items:

- Description of the vulnerability.
- Operating systems/versions affected
- Risks of attempting to exploit (e.g., might crash the host or lock out an account)
- Identify as many attack vectors as you can
- Identify potential blocking mechanisms such as AV software or IDS/IPS, and how you might try to bypass them
- Document how you plan on cracking passwords.
- Remediation action
- CVSS score

Threat Assessment Spreadsheet

Detailed Descriptions

Scenario 1: Unpatched RDP Exposed to the Internet
Scenario 2: Web Application Vulnerable to SQL Injection
Scenario 3: Default Password on Cisco Admin Portal
Scenario 4: Apache Web Server Vulnerability to CVE-2019-0211
Scenario 5: Web Server Exposing Sensitive Data
Scenario 6: Web Application with Broken Access Control
Scenario 7: Oracle WebLogic Server vulnerable to CVE-2020-14882
Scenario 8: Misconfigured cloud storage (AWS security group misconfigurations)
Scenario 9: Microsoft Exchange Server vulnerability
Scenario 10: Windows MSHTML Platform Security Feature Bypass Vulnerability

(See attachment: Phase4_ThreatAssessment.xmls)