Internship details

AD Pentest Automation - Red Team - 2025

Objective:

Develop an automated framework to streamline Active Directory (AD) penetration testing by integrating various assessment tools, aggregating their outputs, and generating comprehensive reports in PwnDoc.

This framework aims to reduce manual effort, improve consistency, and provide actionable insights for Active Directory security evaluations. Authenticated and unauthenticated enum of domain AND also on hosts (like nessus authenticated scan).

Key Responsibilities

1. **Automated Discovery and Enumeration:**
   - Build functionality to accept user-defined scopes (domain names) and credentials (single or multiple users).
   - Automate the execution of discovery tools to identify domain structure, users, groups, and configuration details.
   - Tools to integrate:
     - **NetExec** for lateral movement testing.
     - **PowerView** for reconnaissance and privilege enumeration.
2. **Integration with Advanced Tools:**
   - Leverage **BloodHound** (via its API) to:
     - Automate the import of discovery data.
     - Mark owned accounts and assets.
     - Run predefined queries to identify misconfigurations or vulnerabilities.
   - Use **PingCastle** to perform domain-level health checks and identify potential weaknesses.
3. **Data Aggregation and Parsing:**
   - Collect and normalize output from all integrated tools into a unified format.
   - Identify redundancies, prioritize findings, and categorize issues (e.g., misconfigurations, privilege escalations, exposed credentials).
4. **Reporting and Visualization:**
   - Design a mechanism to export aggregated findings directly into PwnDoc, ensuring clear, actionable, and well-documented reports.
   - Support standardized tagging and categorization of findings for easier triage and remediation.
5. **Framework Design and Extensibility:**
   - Develop the framework primarily in Python (or suggest an alternative language suited to the task).
   - Ensure modularity, enabling easy integration of additional tools or features in the future.

What You'll Learn

1. **Active Directory Penetration Testing:**
   - Gain in-depth knowledge of AD enumeration, privilege escalation, and common misconfigurations.
   - Learn to use tools like PowerView, NetExec, and BloodHound to automate reconnaissance and attack simulations.
2. **Automation and Scripting:**
   - Hands-on experience developing automation scripts in Python, integrating multiple tools and APIs for streamlined workflows.
   - Learn to handle tool outputs (e.g., JSON, XML) and normalize them for reporting.
3. **API Integration and Data Visualization:**
   - Work with REST APIs (e.g., BloodHound, PwnDoc) for automating tasks and creating comprehensive visual reports.
4. **Framework Development:**
   - Design modular, extensible frameworks to integrate additional tools or features for broader AD security testing use cases.
5. **Cybersecurity Reporting and Analytics:**
   - Develop skills in structured reporting and visualization using tools like PwnDoc, ensuring actionable insights for stakeholders.

Preferred Skills and Qualifications

- **Foundational Knowledge:**
  - Basic understanding of Active Directory structures and common vulnerabilities.
  - Familiarity with penetration testing concepts and methodologies.
- **Programming Skills:**
  - Proficiency in Python (or willingness to learn) for scripting and automation.
  - Familiarity with libraries for API handling, data parsing, and scripting (e.g., requests, json).
- **Tool Experience:**
  - Exposure to AD enumeration tools such as BloodHound, PowerView, and PingCastle is a plus.
  - Experience with reporting tools like PwnDoc or similar platforms.
- **Problem-Solving and Analytical Thinking:**
  - Ability to analyze and prioritize findings from multiple sources.
  - Strong debugging skills to handle tool integrations and edge cases.
- **Passion for Learning:**
  - Eagerness to explore cutting-edge technologies in cybersecurity automation and reporting.

Perks and Benefits

1. **Hands-On Experience:**
   - Direct exposure to real-world AD penetration testing tools and scenarios.
   - Opportunity to build and showcase an end-to-end framework for automation and reporting.
2. **Mentorship:**
   - Guidance from cybersecurity professionals with expertise in penetration testing and automation.
3. **Skill Development:**
   - Gain proficiency in tools like BloodHound, NetExec, and PingCastle, and frameworks like PwnDoc.
   - Master advanced scripting and automation concepts.
4. **Flexibility:**
   - Flexible working hours (if applicable) to suit academic or personal schedules.
5. **Career Growth:**
   - Potential for a full-time role upon successful internship completion.
   - Build a portfolio-ready project to showcase during job applications.

Expected Deliverables

1. **A functional wrapper script that automates:**
   - Tool execution based on scope and credentials.
   - Data aggregation and parsing.
   - Querying and updating BloodHound via its API.
2. **Integration with PwnDoc for structured reporting of findings.**
3. **Comprehensive documentation, including:**
   - Usage instructions for testers.
   - Details on adding new tools or extending functionality.
4. **A final presentation showcasing the framework's capabilities and use cases.**

Tools and Technologies

- Programming language: **Python** (preferred) or a suggested alternative.
- Tools for Integration: **NetExec, BloodHound (API), PingCastle, PowerView**, and others as defined during the internship.
- Reporting Tool: **PwnDoc.**
- Libraries/Frameworks:
  - REST APIs (for BloodHound and PwnDoc).
  - Parsing libraries for tool output (e.g., JSON, XML, or text parsers).