The future belongs to those who believe in the beauty of their dreams

Eleanor Roosevelt
Fatma Fouad Yousef

- Bachelor's degree, computer engineering (Kuwait University)

- Senior system engineer at PACI (2012-present)

- Cybersecurity (sec+501)

- Linuxing, lifetime lover of animals, dreamer, Workaholic, Helper.. #speaker #volunteer
Penetration testing

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.
Pentest Methodology

- Planning & Scoping
- Info Gathering & Vulnerability ID
- Attacks & Exploits
- Reporting & Communication
Planning a Penetration Test

• Rules of Engagement

• Determining scope

• Who has the authority to authorize testing? • What is the purpose of the test? • What is the proposed timeframe for the testing? Are there any restrictions as to when the testing can be performed? • Does your customer understand the difference between a vulnerability assessment and a penetration test?
Testing Strategies

- Internals Not Known
- Internals Relevant to Testing Known
- Internals Fully Known
Target Selection

- Internal or External
- Physical
- Users
- SSIDs
- Applications
Information gathering and Vulnerability

• Conducting information gathering
• Performing vulnerability scanning
• Analyzing results of vulnerability scans
Vulnerability Scans

Scans of a host, system, or network to determine what vulnerabilities exist

- Credentialed scans
  - Scanner uses an authorized user or admin account
  - Closer to the system administrator’s perspective
  - Finds more vulnerabilities

- Non-credentialed scans
  - Scanner doesn’t have a user or admin account
  - Closer to the hacker’s perspective
## Analyzing results of vulnerability scans

<table>
<thead>
<tr>
<th>Asset Categorization</th>
<th>Adjudication</th>
<th>Prioritize the Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Categorize by Operating System or function.</td>
<td>Must consider which vulnerabilities to attack</td>
<td>Consider the most critical vulnerabilities first</td>
</tr>
<tr>
<td>Domain Controllers, Web Servers, Databases, etc.</td>
<td>False positives</td>
<td>What target should we focus on first?</td>
</tr>
<tr>
<td>▪ Categorize by most vulnerabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Categorize by the most critical vulnerability</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Attacks and Exploits

Application-based Vulnerabilities

• Cross-site scripting (XSS)
• Clickjacking
• Security misconfiguration (Directory traversal)

• Unsecure coding practices (Unauthorized use of function/unprotected API)

  Designers should implement function-level access control
Cross-Site Request Forgery
Injection Attacks

• Insertion of additional information or code via a data input from a client to the application
• Most commonly done as SQL inject, but can also be HTML, Command, or Code
• Prevent this through input validation and using least privilege for the databases
Authentication

*Session hijacking
Attacks the web session control mechanism by taking over a session by guessing session token

*Redirect

*Default credentials
Reporting and Communication

Communication Paths

Reasons

▪ Situational Awareness
  A shared common understanding of the network and its current security state

▪ De-confliction
  Determining if detected activity is a hacker or an authorized penetration tester
Triggers

• Stages
  Communication often occurs as the assessment moves from one phase to another

IOC
• Indicators of Compromise (IOC) are the evidence that a cyber-attack has taken place.
• IOC give valuable information about what has happened but can also be used to prepare for the future and prevent against similar attacks.
• Critical findings
Report writing and handling best practices

• Normalization of Data
• Written Report of Findings
• How Long Do I Keep the Report?
Mitigation Strategies

Report should contain a list of not just findings, but recommendations on how to mitigate a vulnerability

• Technology
  o Add a multifactor authentication system

• People
  o Employee cybersecurity training
  o Hire qualified and certified IT professionals
Post-Report Activities

- Post-Engagement Cleanup • Remove shells, tools, and credentials created
- Client Acceptance • Does the client agree you have fulfilled the scope of work?
- Follow-up Actions or Retests • Will a retest be conducted after 30 or 90 days?
Lessons learned

• If both positive and negative experience occurred.
• How can it go better next time.
• What did you do great on!
• What could have gone better!
Thank you