Phase 3: Identify Vulnerabilities

Goal: Identify the tools and techniques to be used to scan for vulnerabilities.

Procedure: List out the tools you plan on using to perform vulnerability scanning and how you will use them. Include both Tenable Nessus and OpenVAS. Remember to include tools designed to look for vulnerabilities within specific technologies or platforms, such as Cisco devices, remote access services, and web applications (e.g., Burp Suite). Follow the same documentation procedure you performed in the previous step. Include screenshots of such tools showing configuration options and settings. Finally, list the pros and cons of each tool.

1. Nessus

With Nessus I can scan systems for vulnerabilities and check whether the systems in the network have the latest software patches.

Pros

- Easy and flexible reporting which you can customize your own way.
- Vulnerability scanning of network including IPv4 network ,IPv6 network
- You can scan all common companies' network devices, all common virtualization companies' platforms, and all the operating systems, etc.

Cons

- GUI can crash sometimes.
- Sort’ve expensive unless financed by an organization.
- Sometime Scans takes a little bit longer then expected

2. OpenVAS

OpenVAS can be used to actively detect thousands of vulnerabilities in network services such as SMTP, DNS, VPN, SSH, RDP, VNC, HTTP, and many more. OpenVAS does vulnerability detection by connecting to each network service and sending crafted packets to make them respond in certain ways.

Pros

- The scan engine of OpenVAS is updated on a regular basis
- Greenbone provides thorough tutorials for the usage of this tool
- Built to be an all-in-one scanner

Cons

- Covers fewer CVEs as compared to Nessus
- Less operating system supportability
- Does not offer policy management

3. Burp Suite

I will use Burp Suite to scan websites for vulnerabilities.

Pros
- Manual penetration testing and configuration tweaks
- Automated bulk scanning and simulated scenarios
- Inspection/altering of HTTPb requests/responses.

Cons
- More comprehensive integration with government regulations would help in terms of compliance efforts.
- The interface is outdated and uses tabs for everything, can get lost in deep nested features if you're new

4. Metasploit

Metasploit will be used to probe systematic vulnerabilities on networks and servers.

Pros
- Updated databases of exploits
- Very intuitive interface and searching
- Community driven: Many developers from all over the world contribute to Metasploit. This helps to keep it functioning well and up-to-date.

Cons
- Can't use it in a active environment or you might damage something.
- If not handled safely, it can crash the system.

5. Netsparker

Netsparker is a dead accurate automated scanner that will identify vulnerabilities such as SQL Injection and Cross-site Scripting in web applications and web APIs.

Pros

- Netsparker has a selection of workflows and integration tools that make it useful for keeping all of my teammates on the same page.
- NetSparker is very user-friendly. It's UI is organized and keeps all the different scans we have set-up in a very clean visual.

  Cons
- NetSparker is priced at a higher range
- It can eat up resources sometimes