SSN College of Engineering,
Department of Computer Science and Engineering
IT8761 Security Laboratory

Exercise 11:

AIM:
To download the N-Stalker Vulnerability Assessment Tool and exploring the features.
Output: Snapshots captured at each and every step of the operations mentioned under Hints

EXPLORING N-STALKER:

- N-Stalker Web Application Security Scanner is a Web security assessment tool.
- It incorporates with a well-known N-Stealth HTTP Security Scanner and 35,000 Web attack signature database.
- This tool also comes in both free and paid version.
- Before scanning the target, go to "License Manager" tab, perform the update.
- Once update, you will note the status as up to date.
- You need to download and install N-Stalker from www.nstalker.com.

Hints:

1. Start N-Stalker from a Windows computer. The program is installed under Start ⇨ Programs ⇨ N-Stalker ⇨ N-Stalker Free Edition.
2. Enter a host address or a range of addresses to scan.
3. Click Start Scan.
4. After the scan completes, the N-Stalker Report Manager will prompt
5. Select a format for the resulting report as choose Generate HTML.
6. Review the HTML report for vulnerabilities.
7. Now goto "Scan Session", enter the target URL.
   In scan policy, you can select from the four options,
   - Manual test which will crawl the website and will be waiting for manual attacks.
   - full xss assessment
   - owasp policy
   - Web server infrastructure analysis.
8. Once, the option has been selected, next step is "Optimize settings" which will crawl the whole website for further analysis.
9. In review option, you can get all the information like host information, technologies used, policy name, etc.
10. Once done, start the session and start the scan.

The scanner will crawl the whole website and will show the scripts, broken pages, hidden fields, information leakage, web forms related information which helps to analyze further.

Once the scan is completed, the NStalker scanner will show details like severity level, vulnerability class, why is it an issue, the fix for the issue and the URL which is vulnerable to the particular vulnerability?