Assignment 8

Title: Implementation of IT Audit, Malware analysis and Vulnerability assessment and generate the report.

Theory:
Vulnerability Analysis tool:

1. **Nikto**

   nikto -h

   nikto -H

   nikto -h www.thisisleagal.com -Tuning x (-h: specifies the target host and x: specifies the Reverse Tuning Options (i.e., include all except specified)

-Tuning

Tuning options will control the test that Nikto will use against a target. A tuning scan can be used to decrease the number of tests performed against a target. By specifying the type of test to include or exclude, faster and focused testing can be completed. This is useful in situations where the presence of certain file types such as XSS or simply "interesting" files is undesired.

By default, if any options are specified, only those tests will be performed. If the "x" option is used, it will reverse the logic and exclude only those tests. Use the reference number or letter to specify the type, multiple may be used:

- **0 – File Upload**

- **1 – Interesting File / Seen in logs**
- **2 – Misconfiguration / Default File**
- **3 – Information Disclosure**
- **4 – Injection (XSS/Script/HTML)**
- **5 – Remote File Retrieval – Inside Web Root**
- **6 – Denial of Service**
- **7 – Remote File Retrieval – Server Wide**
- **8 – Command Execution / Remote Shell**
- **9 – SQL Injection**
- **a – Authentication Bypass**
- **b – Software Identification**
- **c – Remote Source Inclusion**
- **x – Reverse Tuning Options (i.e., include all except specified)**

The given string will be parsed from left to right, any x characters will apply to all characters to the right of the character.

So, to only perform an SQL injection test against your target:

nikto -Tuning 9 -h example.com

or to run everything except DOS

nikto -Tuning x 6 -h example.com

nikto -h www.thisislegal.com -o outputnikto -F txt

-h: specifies the target, -o: specifies the name of the output file, and -F: specifies the file format.

output file:

- Nikto v2.1.6/2.1.5

+ Target Host: www.thisislegal.com

+ Target Port: 80

+ GET The anti-clickjacking X-Frame-Options header is not present.

(the server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>.)

+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

(The `X-XSS-Protection` header is designed to 0

+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ OSVDB-637: GET Enumeration of users is possible by requesting ~username (responds with 'Forbidden' for users, 'not found' for non-existent users).

+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST

Malware analysis

Wireshark

1. Open wireshark, right click to eth0 and hit on start capture (pcap- packet capture)
2. select your ip and apply filter
3. Now close the current window and come back to wireshark window
4. write targeted URL inside the text box (filter)

   example: http://testphp.vulnweb.com/login.php

1. Start pcap
2. goto browser and write http://testphp.vulnweb.com/login.php
3. enter any username and password
4. come back to wireshark, stop pcap.
5. add filter as http.request.method=="GET"
6. http.request.method=="POST"
   U CAN CHECK YOUR CREDENTIALS UNDER

html form URL encoded.

Conclusion:

FAQs

1. **Detailing of output file "outputnikto".**
2.