Beykoz University

Department of “Computer Engineering”

“Information Systems Security - 60619MEEOZ-CME0147”

Penetration Test Project

- Interim Report -

Lecturer: DUYGU DEMİRAY

Leyla Abdullayeva - 1904010038

Little information about project:

What is Kali Linux?

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering. I'll also use this for my project and also I'll use tools of Kali Linux. Kali.org has recently released its new update with some extra functionalities. There are different types of tools that are present in Kali Linux to perform different operations.

The tool that I'll definitely use:

Web Application Analysis

Web Application is a dynamic response web page that helps in a better and interactive client-server relationship. These tools identify and access websites through the browser to check any bug or loophole present, which could lead any information or data to be lost. For example, there is a website with a payment gateway then these web analyzers check if sufficient authentication and authorization present of the site. These web application uses:

SQL injections
Denial of service
URL manipulation

Some of the tools are:
Burpsuite
Httrack
Sqlmap
Vega
Webscarab
Wpscan
Burpsuite, vega, and web scarab.

Steps that I'll follow:

I'm planning to use "skipfish" which is already online tool and has documentation on Kali.org. here's the link:
https://www.kali.org/tools/skipfish/

skipfish Usage Example

Using the given directory for output (`-o 202`), scan the web application URL (`http://192.168.1.202/wordpress`):

```
root@kali:~# skipfish -o 202 http://192.168.1.202/wordpress

skipfish version 2.10b by lcamtuf@google.com

  - 192.168.1.202 -

Scan statistics:

      Scan time : 0:00:05.849
  HTTP requests : 2841 (485.6/s), 1601 kB in, 563 kB out (370.2 kB/s)
    Compression : 802 kB in, 1255 kB out (22.0% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 46 total (61.8 req/conn)
     TCP faults : 0 failures, 0 timeouts, 16 purged
 External links : 512 skipped
   Reqs pending : 0

Database statistics:

         Pivots : 13 total, 12 done (92.31%)
    In progress : 0 pending, 0 init, 0 attacks, 1 dict
  Missing nodes : 0 spotted
     Node types : 1 serv, 4 dir, 6 file, 0 pinfo, 0 unkn, 2 par, 0 val
   Issues found : 10 info, 0 warn, 0 low, 8 medium, 0 high impact
      Dict size : 20 words (20 new), 1 extensions, 202 candidates
     Signatures : 77 total

[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 13
[+] Looking for duplicate entries: 13
[+] Counting unique nodes: 11
[+] Saving pivot data for third-party tools...
[+] Writing scan description...
[+] Writing crawl tree: 13
```

Web Penetration Testing Tools

1. Burp Suite

Burp Suite is one of the most popular web application security testing software. It is used as a proxy, so all the requests from the browser with the proxy pass through it.

2. Nikto

Nikto is an Open Source software written in Perl language that is used to scan a web-server for the vulnerability that can be exploited and can compromise the server.

3. Maltego

Maltego is a platform developed to convey and put forward a clear picture of the environment that an organization owns and operates.

4.SQL Map

SQLMap is an open-source tool that is used to automate the process of manual SQL injection over a parameter on a website.

5. Whatweb

Whatweb is an acronym of “what is that website“.It is used to get the technologies which a website is using, these technologies might me content management system(CMS), Javascript Libraries, etc.

6. whois lookup

whois is a database record of all the registered domain over the internet.

REFERENCES:

https://www.kali.org/tools/skipfish/

https://www.geeksforgeeks.org/kali-linux-web-penetration-testing-tools/

https://www.geeksforgeeks.org/kali-linux-tools/#web

https://www.javatpoint.com/kali-linux-web-application-tools

https://www.tutorialspoint.com/kali_linux/kali_linux_website_penetration_testing.htm