

Vulnerability Scanning Lab

Table of contents

- **Overview**
- **Effectiveness of Applications**
- **Potential Vulnerabilities** (Nmap -p- -A #, Kioptrix 3 website, Kioptrix 3 website source page, Nikto, OWASP ZAP)
- **Dangerous Website Extensions**
- **Defensive Strategy**
- **Summary**
- **Screenshots**
- **Reference Page**

Overview:

In this lab, we practiced the basics of vulnerability scans first by practicing with Kioptrix 2, with step-by-step instructions, then worked with kioptrix 3 as a homework assignment. We used multiple types of vulnerability scans such as Nmap, Nikto, and OWASP Zap, to assist us in areas where a website could be attacked. The intention of this was to identify potential access points. This would be used when being asked by an employer where a site could be vulnerable to an attack.

Effectiveness of Applications:

The potential effects could be damaging to multiple different institutions. Companies that work in finance, government, or commerce should be some of the first to instantly have a cybersecurity team run some kind of vulnerability scan on their networks. These sectors are trusted with critical information that many trust them with. If their networks happen to be vulnerable and

leave some kind of information that would gain access to a private space, that trust many had could quickly disappear. A Cyber Security team would quickly cut the loose ends of the security system put into place and only reinforce it for the better.

Potential Vulnerabilities:

Nmap: Will instantly reveal which ports are unsecured, which only reveals a vulnerability and a place to start. Provides information on what kind of attacks can potentially work such as MySQL, CentOS, Apache, and more if revealed.

Kioptrix 3 Website: Cannot successfully reveal a vulnerability by triggering access codes.

Kioptrix 3 Source Page: Reveals potential vulnerabilities such as the programs used which could be used as a starting point to gain access to the system.

Nikto: Picks up server information, in this case, reveals the use of Apache. Reveals that the anticlickjack X header is not present. Reveals that the X-XSS Protection Header is not defined. Shows that certain HTTP requests could also allow access to the network.

Owasp Zap: Used to perform automated scans that perform attacks that will provide all sorts of data and ways into the system. The intention of this system is to reveal vulnerabilities that would allow others access to the system.

Dangerous Website Extensions:

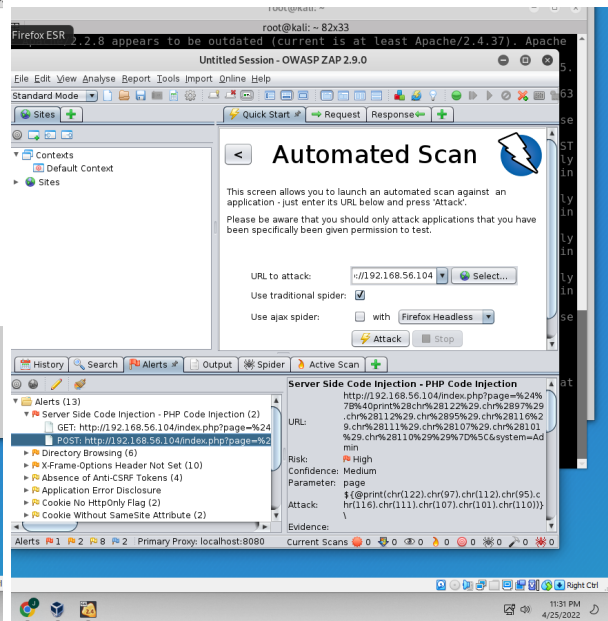
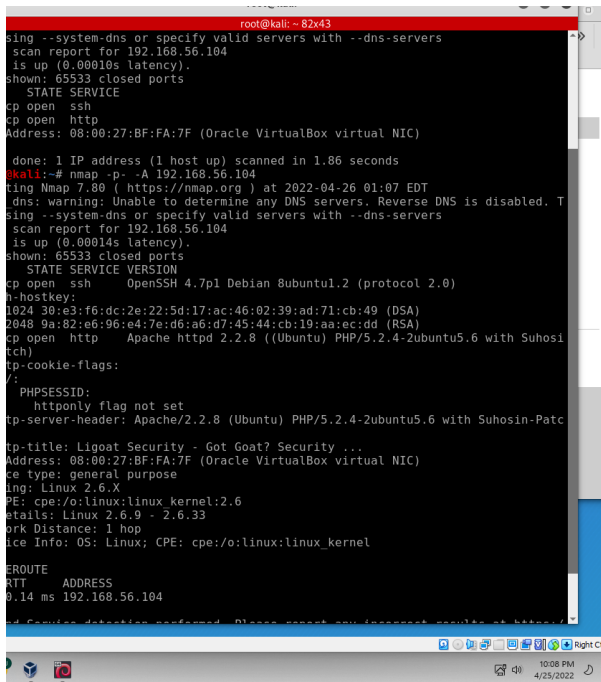
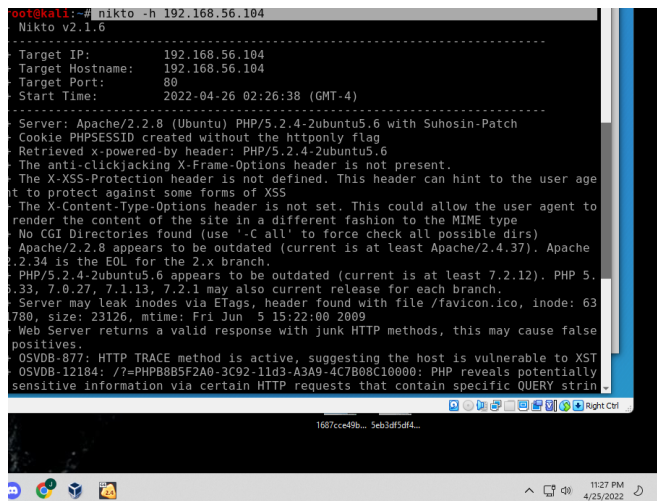
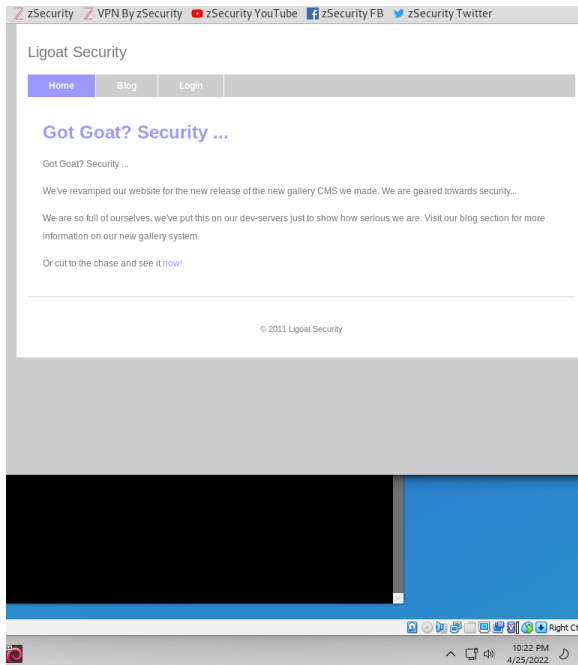
SQL Injection: This attack inserts an SQL script, which is a language used by most databases to perform quarry operations. This attack enables most attackers to pass many things such as login screenshots and access sensitive databases. Most apps are protected against attacks like this but when this vulnerability is found, it could be malicious.

Code Injection: One of the most common attacks to take place, attackers must know the programming language that the program is written in. They can inject code into certain areas to force the web observer they are looking for. This attack requires someone to not only know the network they are trying to access quite well but the programming language as well.

Defensive Strategy: When it comes to defensive strategies, you really have to build up a system around what you are trying to prevent. For SQL scripts, it is very important for the system not to be developed to be penetrated by SQL scripts. Most programs are far past being disturbed by my SQL scripts. As for code injections, it is crucial for the code writers to be tight with their code. If you write code that has multiple loose ends that could simply be dissected by a person that knows the same coding language as you, it's probably a satisfactory job.

Summary: In conclusion, vulnerability testing is a crucial role in the cybersecurity world. There are many tests we can run that will reveal what kind of vulnerabilities systems and networks expose themselves to for attacks. This lab taught us a few of the tests we might run so the vulnerabilities could expose themselves.

Screenshots:



```
root@kali: ~
OS and Service detection performed. Please report any incorrect results at https://
/nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 9.64 seconds
root@kali:~# dirb http://192.168.56.104

-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Tue Apr 26 01:10:48 2022
URL BASE: http://192.168.56.104/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

---- Scanning URL: http://192.168.56.104/ ----
==> DIRECTORY: http://192.168.56.104/cache/
+ http://192.168.56.104/data (CODE:403|SIZE:325)
+ http://192.168.56.104/favicon.ico (CODE:200|SIZE:23126)
==> DIRECTORY: http://192.168.56.104/gallery/
+ http://192.168.56.104/index.php (CODE:200|SIZE:1819)
==> DIRECTORY: http://192.168.56.104/modules/
+ http://192.168.56.104/phpmyadmin/
+ http://192.168.56.104/server-status (CODE:403|SIZE:334)
==> DIRECTORY: http://192.168.56.104/style/

---- Entering directory: http://192.168.56.104/cache/ ----
+ http://192.168.56.104/cache/index.html (CODE:200|SIZE:1819)

---- Entering directory: http://192.168.56.104/core/ ----
==> DIRECTORY: http://192.168.56.104/core/controller/
+ http://192.168.56.104/core/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.56.104/core/lib/
==> DIRECTORY: http://192.168.56.104/core/model/
==> DIRECTORY: http://192.168.56.104/core/view/

---- Entering directory: http://192.168.56.104/gallery/ ----
+ http://192.168.56.104/gallery/index.php (CODE:500|SIZE:5650)
==> DIRECTORY: http://192.168.56.104/gallery/photos/
+ http://192.168.56.104/gallery/photos/1.jpg (CODE:200|SIZE:102400)
```

```
1 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
2 <!-- [endif] -->
3 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
4 <!-- [endif] -->
5 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
6 <!-- [endif] -->
7 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
8 <!-- [endif] -->
9 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
10 <!-- [endif] -->
11 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
12 <!-- [endif] -->
13 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
14 <!-- [endif] -->
15 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
16 <!-- [endif] -->
17 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
18 <!-- [endif] -->
19 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
20 <!-- [endif] -->
21 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
22 <!-- [endif] -->
23 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
24 <!-- [endif] -->
25 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
26 <!-- [endif] -->
27 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
28 <!-- [endif] -->
29 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
30 <!-- [endif] -->
31 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
32 <!-- [endif] -->
33 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
34 <!-- [endif] -->
35 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
36 <!-- [endif] -->
37 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
38 <!-- [endif] -->
39 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
40 <!-- [endif] -->
41 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
42 <!-- [endif] -->
43 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
44 <!-- [endif] -->
45 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
46 <!-- [endif] -->
47 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
48 <!-- [endif] -->
49 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
50 <!-- [endif] -->
51 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
52 <!-- [endif] -->
53 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
54 <!-- [endif] -->
55 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
56 <!-- [endif] -->
57 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
58 <!-- [endif] -->
59 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
60 <!-- [endif] -->
61 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
62 <!-- [endif] -->
63 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
64 <!-- [endif] -->
65 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
66 <!-- [endif] -->
67 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
68 <!-- [endif] -->
69 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
70 <!-- [endif] -->
71 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
72 <!-- [endif] -->
73 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
74 <!-- [endif] -->
75 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
76 <!-- [endif] -->
77 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
78 <!-- [endif] -->
79 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
80 <!-- [endif] -->
81 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
82 <!-- [endif] -->
83 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
84 <!-- [endif] -->
85 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
86 <!-- [endif] -->
87 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
88 <!-- [endif] -->
89 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
90 <!-- [endif] -->
91 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
92 <!-- [endif] -->
93 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
94 <!-- [endif] -->
95 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
96 <!-- [endif] -->
97 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
98 <!-- [endif] -->
99 <!-- [if IE] <img alt="Ligat Security Logo" data-bbox="120 410 200 430" />
100 <!-- [endif] -->
```

Reference Page:

Top 20 most common types of cyber attacks. Fortinet. (n.d.). Retrieved April 26, 2022, from <https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks>