

# BIS\_Lab\_4\_427008954

*by* Naresh Choudhary

---

**Submission date:** 14-Feb-2019 11:38PM (UTC-0600)

**Submission ID:** 1078562592

**File name:** BIS\_LAB\_4.docx (902.94K)

**Word count:** 429

**Character count:** 2874

## Business Information Security Lab 4

### Task 1:

Two vulnerability scanner tools on Kali Linux:

1. OpenVAS
2. Sparta

Tool for web application analysis:

1. OWASP ZAP

### Task 2:

**Documentation link for OpenVAS:** <http://openvas.org/>

**Documentation link for Sparta:** <http://sparta.secforce.com/documentation/>

**Documentation link for OWASP ZAP:** [www.owasp.org/index.php/OWASP Zed Attack Proxy Project](http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)

## Business Information Security Lab 4

### Task 4:

#### (A) Scan results of Sparta & OpenVAS

##### 1. Sparta result shows two passwords.

SPARTA 1.0.3 (BETA) - untitled - /root/

Target	Port
192.168.80.136	21/tcp
192.168.80.136	2121/tcp

Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or

Hydra (http://www.thc.org/thc-hydra) starting at 2019-02-13 17:52:13  
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries, ~1 try per task  
[DATA] attacking ftp://192.168.80.136:21/  
[21][ftp] host: 192.168.80.136 login: ftp password: password  
[STATUS] attack finished for 192.168.80.136 (valid pair found)  
**1 of 1 target successfully completed, 1 valid password found**  
Hydra (http://www.thc.org/thc-hydra) finished at 2019-02-13 17:52:14

SPARTA 1.0.3 (BETA) - untitled - /root/

Target	Port
192.168.80.136	5432/tcp

Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizat

Hydra (http://www.thc.org/thc-hydra) starting at 2019-02-13 17:52:07  
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries, ~1 try per task  
[DATA] attacking postgres://192.168.80.136:5432/  
**[5432][postgres] host: 192.168.80.136 login: postgres password: postgres**  
1 of 1 target successfully completed, 1 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2019-02-13 17:52:07

Hosts Services Tools Services Scripts Information Notes nikto (80/tcp) screenshot (80/tcp) smtp-enum-vrfy (25/tcp) mysql-default

OS	Host
192.168.80.136	

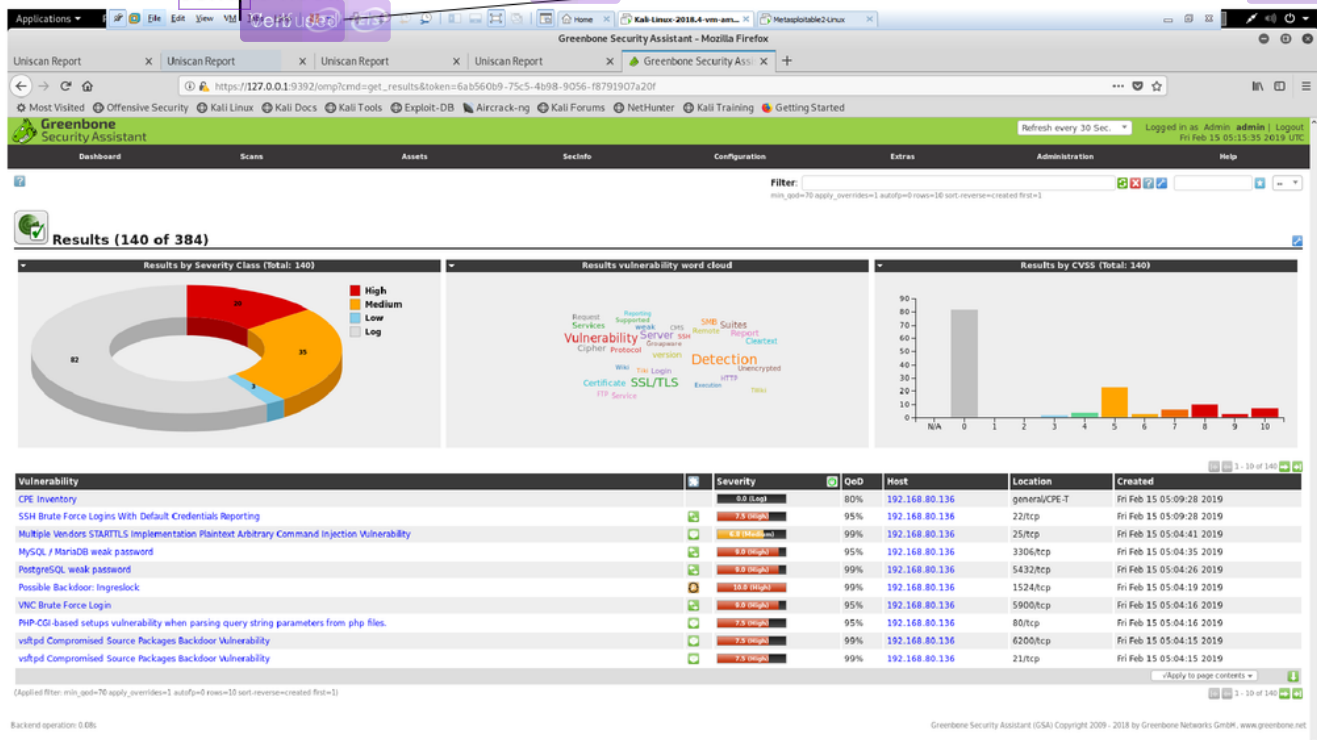
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2019-02-13 17:52:07

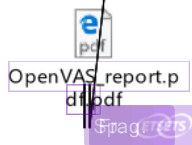
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)  
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3 login tries, ~1 try per task  
[DATA] attacking mysql://192.168.80.136:3306/  
[3306][mysql] host: 192.168.80.136 login: root  
[STATUS] attack finished for 192.168.80.136 (valid pair found)  
1 of 1 target successfully completed, **1 valid password found**  
Hydra (http://www.thc.org/thc-hydra) finished at 2019-02-13 17:52:07

## Business Information Security Lab 4

2. OpenVas shows 140 vulnerabilities based on priority. High priority vulnerabilities included use of DistCC 2.x, running of rlogin service, vsftpd (prone to backdoor hack), rexec service. OpenVas report (attached) shows the default username and password of Metasploit2. Many unspecified SQL-injection vulnerabilities were found. Further, Web servers were misconfigured resulting in dangerous HTTP PUT and delete message be send to host.

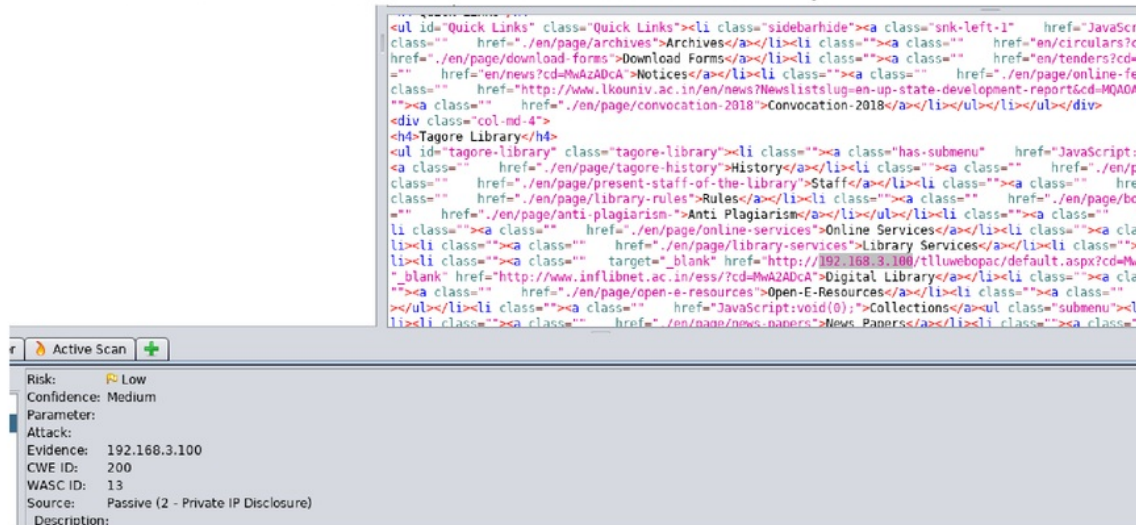


Detailed report:

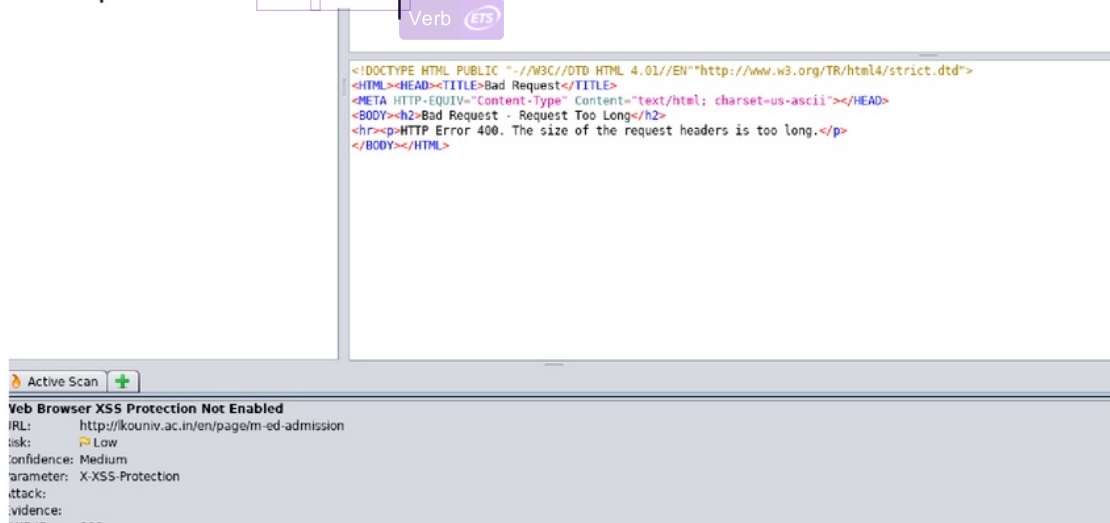


**(B) Scan results for OWASP ZAP (Scan results of url lkouniv.ac.in):**

- A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) was found in a response body. Internal servers ip can help hacker to attack the same or find a link to enter into the system.



- XSS protection is disabled. It can cause hacker to run unauthorized scripts



- An attacker can access files, directories and commands that are potentially dangerous using Path Traversal attack technique. Contents that are sensitive can be accessed by manipulate a URL. Usually web sites restrict access to "web document root" or "CGI root" directory. These directories contain the files that are used by user access and the executable used for web apps functions. It uses special-character "/" to alter the resource location requested in the URL.

## Business Information Security Lab 4

A web app can be vulnerable due to improper handling of user-supplied input.

```
building will be ready by Dec. 2019.</p>
<p>Faculty of Engineering is located in the second campus of the University in Jankipuram. It
accommodates Faculty of Law, Faculty of Management and several other professional courses in
addition to Faculty of Engineering. Large stretches of this area is covered by green belt. The
Eco-friendly practices and teaching, learning are planned to be combined together to promote
sustainable development. Furthermore, initiatives have also been taken towards energy
conservation and tapping of solar energy in the campus.</p>
</div>
</div>
</div>
<div class="panel panel-default">
<div class="panel-heading" role="tab" id="heading2">
<h4 class="panel-title"><a class="collapsed" role="button" data-toggle="collapse" data-parent=
"#accordion" href="#collapse2" aria-expanded="false" aria-controls="collapse2"> <i class=
"more-less glyphicon glyphicon-plus pull-right"></i> ADMISSIONS</a></h4>
</div>
```

Active Scan +

**Path Traversal**

URL: http://lkouniv.ac.in/en/page/faculty-of-engineering?query=c%3A%2F

Risk: High

Confidence: Medium

Parameter: query

Attack: c:/

Evidence: etc

WE ID: 22

**Task 5:**

Scan from sparta found 3 username and passwords of Metasploit2. These are the default username and passwords set while installing Metasploit2. These include ftp, postgresql and SQL passwords. Using these hackers can perform SQL injection to hack, corrupt or service denial. Older version of PHP were detected which are prone to an information-disclosure vulnerability. It could have been updated to PHP version 5.4+ (which is recommended by PHP). Similarly, older version of Ruby permits unauthorized systems to execute commands dangerous to system. Reports from OpenVAS shows the extract version of SQL through which unattended vulnerabilities can be exploited.

Similarly for web scanning of lkouniv.ac.in, private IP addresses, path traversal technique and sql injection can be performed. Moreover in html pages, JavaScript can be written to access internal information. There should be a filter which doesn't allow JavaScript codes to run which are embedded in html pages. Similarly XSS protector is present which could be used to input unauthorized commands.



### FINAL GRADE

16/20

### GENERAL COMMENTS

#### Instructor

Task 5 is incomplete as per the rubric Student's assessment of the cybersecurity risk to (a) Metasploitable2 and (b) lkouniv.ac.in from network based attack? a. Your answer provides specific vulnerabilities that can be exploited by an attacker from any remote location. [Maximum 3 Points] b. Your answer provides details (in layman's terms) on how the vulnerabilities can be exploited. [Maximum 3 Points] c. You provide some information on how easy or difficult it is to exploit these vulnerabilities. [Maximum 3 Points] d. You have cited all sources of information in answering this question. [Maximum 1 Point]

PAGE 1

PAGE 2

PAGE 3



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Confused** You have a spelling mistake near the word **of** that makes **of** appear to be a confusion word error.



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Sentence Cap.** Remember to capitalize the first word of each sentence.



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.





**Article Error** You may need to use an article before this word.



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Article Error** You may need to use an article before this word.



**Confused** You have used **send** in this sentence. You may need to use **sent** instead.



**Verb** This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Frag.** This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

PAGE 4

---



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Proofread** This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.



**Verb** This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.



**Article Error** You may need to use an article before this word.



**Article Error** You may need to use an article before this word. Consider using the article **the**.



**Confused** You have used **a** in this sentence. You may need to use **an** instead.



**Proofread** This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.



**Proofread** This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.



**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Article Error** You may need to use an article before this word.



**S/V** This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.



**Article Error** You may need to remove this article.



**P/V** You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.



**Article Error** You may need to use an article before this word.



**Article Error** You may need to use an article before this word.



**Sp.** This word is misspelled. Use a dictionary or spellchecker when you proofread your work.



**Missing ","** You may need to place a comma after this word.



**Article Error** You may need to use an article before this word.