



Information Assurance & Auditing

4th Year - 1st Semester\

Assignment

Registration No : IT 17002448
Name : P. N Dassanaïke
Batch : CSNE - WE

Table of Contents

Introduction	3
SLIIT web site penetration testing using NMAP	4
Site-Performance checker using SEO (semrush tool)	8
Problem Identification.....	11
Recommendations	12
References	13

Introduction

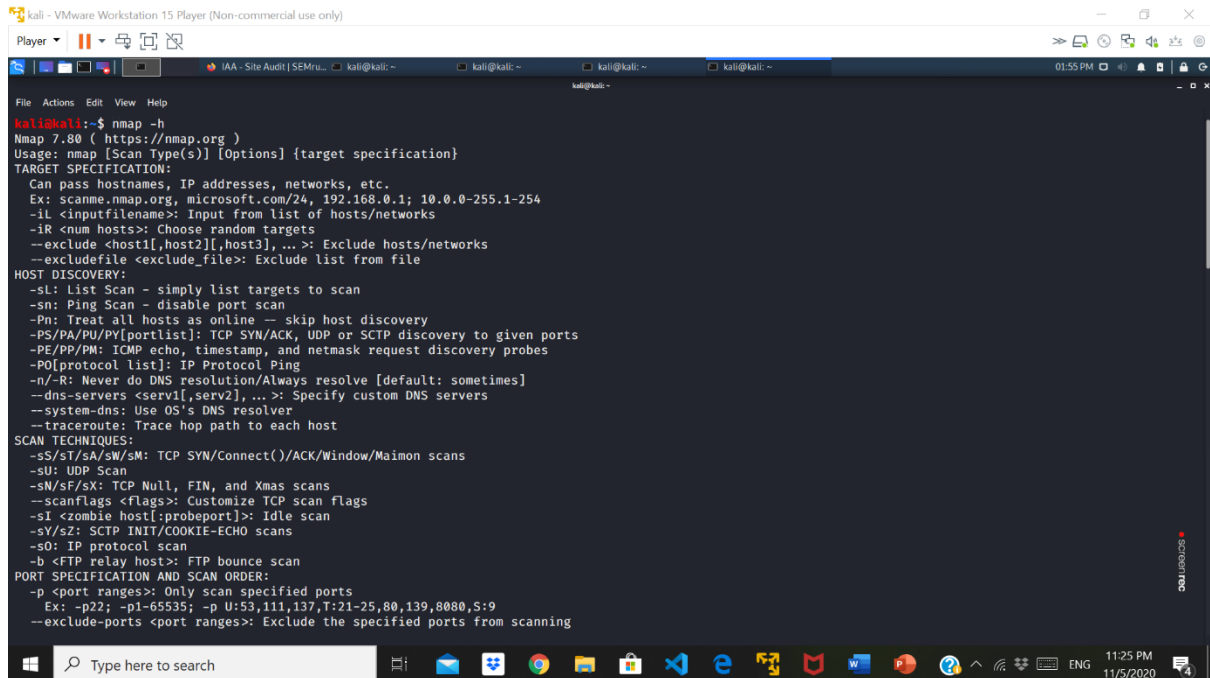
In today's world's websites are the most widely used platform everything and because of that we should do security auditing's regular. So, the best way to do the security auditing is using Vulnerability assessments. So, this report includes the web application penetration testing using NMAP and web site perform testing using SEO audit.

What is Vulnerability Analysis?

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

SLIIT web site penetration testing using NMAP

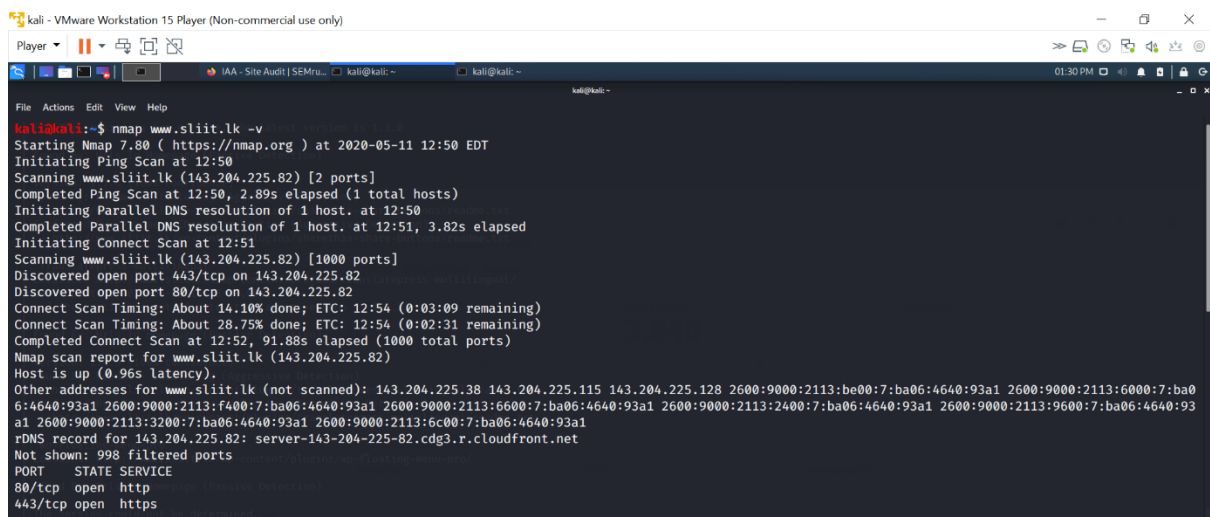
We are using NMAP which is open source for the slit.lk site auditing. First we need to open up the terminal in Kali Linux.



```
kali@kali:~$ nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan type(s)] [Options] [target specification]
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludedfile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sV/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
```

Check IP address and Open port using following command.

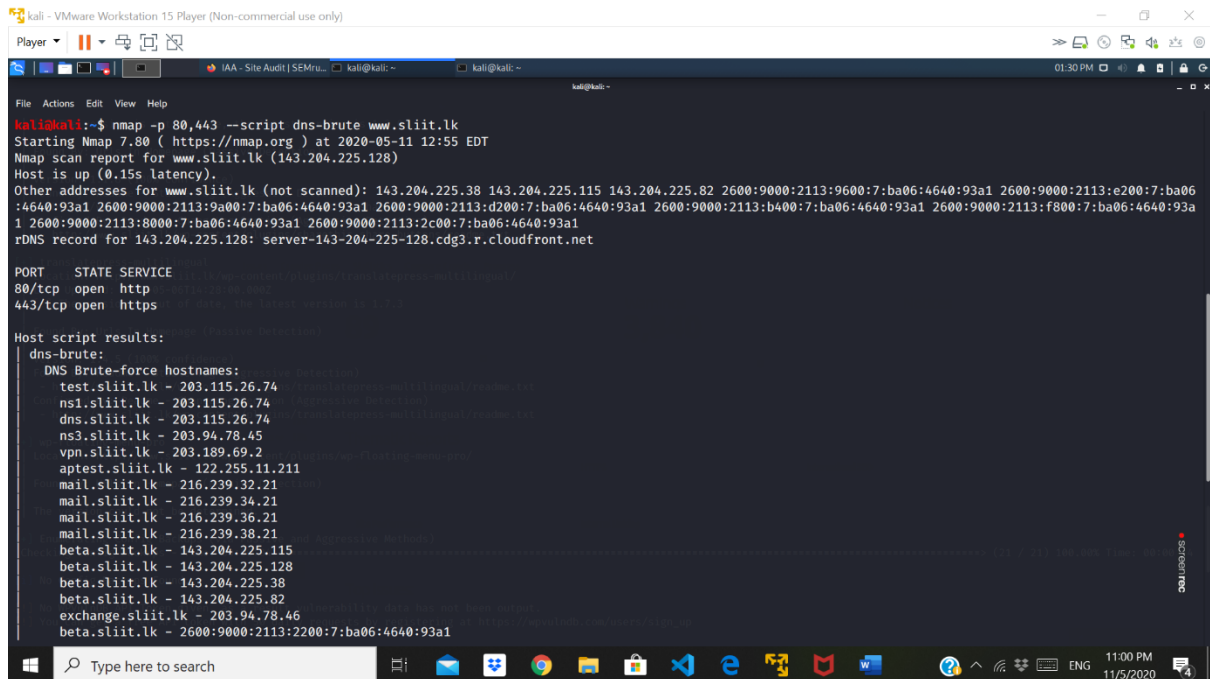
`$ nmap www.sliit.lk`



```
kali@kali:~$ nmap www.sliit.lk -v
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 12:50 EDT
Initiating Ping Scan at 12:50
Scanning www.sliit.lk (143.204.225.82) [2 ports]
Completed Ping Scan at 12:50, 2.89s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:50
Completed Parallel DNS resolution of 1 host. at 12:51, 3.82s elapsed
Initiating Connect Scan at 12:51
Scanning www.sliit.lk (143.204.225.82) [1000 ports]
Discovered open port 443/tcp on 143.204.225.82
Discovered open port 80/tcp on 143.204.225.82
Connect Scan Timing: About 14.10% done; ETC: 12:54 (0:03:09 remaining)
Connect Scan Timing: About 28.75% done; ETC: 12:54 (0:02:31 remaining)
Completed Connect Scan at 12:52, 91.88s elapsed (1000 total ports)
Nmap scan report for www.sliit.lk (143.204.225.82)
Host is up (0.96s latency).
Other addresses for www.sliit.lk (not scanned): 143.204.225.38 143.204.225.115 143.204.225.128 2600:9000:2113:be00:7:ba06:4640:93a1 2600:9000:2113:6000:7:ba06:4640:93a1 2600:9000:2113:f400:7:ba06:4640:93a1 2600:9000:2113:6600:7:ba06:4640:93a1 2600:9000:2113:2400:7:ba06:4640:93a1 2600:9000:2113:9600:7:ba06:4640:93a1
rDNS record for 143.204.225.82: server-143-204-225-82.cdg3.r.cloudfront.net
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

```
kali - VMware Workstation 15 Player (Non-commercial use only)
Player ▾ || 🔊 🔄 🏠
IAA - Site Audit | SEMrush... kali@kali:~ kali@kali:~
kali@kali:~$ nmap -sV -sC www.sliit.lk
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 12:52 EDT
Failed to resolve "www.sliit.lk".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 20.92 seconds
kali@kali:~$ nmap -sV -sC www.sliit.lk
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 12:53 EDT
Nmap scan report for www.sliit.lk (143.204.225.82)
Host is up (6.94s latency).
Other addresses for www.sliit.lk (not scanned): 143.204.225.115 143.204.225.128 143.204.225.38 2600:9000:2113:c200:7:ba06:4640:93a1 2600:9000:2113:2c00:7:ba06:4640:93a1 2600:9000:2113:600:7:ba06:4640:93a1 2600:9000:2113:6c00:7:ba06:4640:93a1 2600:9000:2113:4600:7:ba06:4640:93a1 2600:9000:2113:cc00:7:ba06:4640:93a1 2600:9000:2113:ee00:7:ba06:4640:93a1
rDNS record for 143.204.225.82: server-143-204-225-82.cdg3.r.cloudfront.net
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      Amazon CloudFront httpd
http-cookie-flags:
/:
PHPSESSID:
- httponly flag not set
http-robots.txt: 54 disallowed entries (15 shown)
/cgi-bin/ /wp-admin/
https://www.sliit.lk/business/staff/lakshman.a /science-education/ /engineering/staff/chandana.p/
/business/staff/wasantha.r/ /engineering/staff/amali.p/
/web-site-is-maintain-mode/ /my-profile/ /profile-computing/
/blog/computing-news/18268/ /profile-business/ /profile-engineering/
/profile-graduate-studies/ /category/blog/fccc/
http-server-header:
CloudFront
nginx/1.10.3 (Ubuntu)
http-title: Did not follow redirect to https://www.sliit.lk/
443/tcp   open  ssl/http  Amazon CloudFront httpd
http-cookie-flags:
/:
PHPSESSID:
- httponly flag not set
```

Next check-up the subdomain of the site.

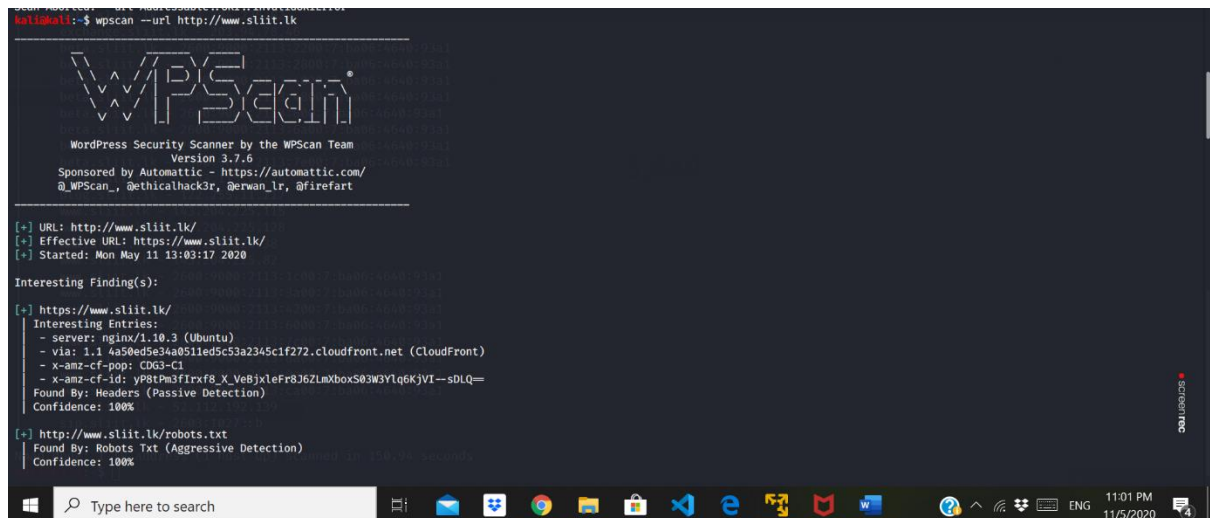


```
kali@kali:~$ nmap -p 80,443 --script dns-brute www.sliit.lk
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 12:55 EDT
Nmap scan report for www.sliit.lk (143.204.225.128)
Host is up (0.15s latency).
Other addresses for www.sliit.lk (not scanned): 143.204.225.38 143.204.225.115 143.204.225.82 2600:9000:2113:9600:7:ba06:4640:93a1 2600:9000:2113:e200:7:ba06:4640:93a1 2600:9000:2113:9a00:7:ba06:4640:93a1 2600:9000:2113:d200:7:ba06:4640:93a1 2600:9000:2113:b400:7:ba06:4640:93a1 2600:9000:2113:f800:7:ba06:4640:93a1 2600:9000:2113:8000:7:ba06:4640:93a1 2600:9000:2113:2c00:7:ba06:4640:93a1
rDNS record for 143.204.225.128: server-143-204-225-128.cdg3.r.cloudfront.net

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Host script results:
dns-brute:
DNS Brute-force hostnames:
test.sliit.lk - 203.115.26.74
ns1.sliit.lk - 203.115.26.74
dns.sliit.lk - 203.115.26.74
ns3.sliit.lk - 203.94.78.45
vpn.sliit.lk - 203.189.69.2
aptest.sliit.lk - 122.255.11.211
mail.sliit.lk - 216.239.32.21
mail.sliit.lk - 216.239.34.21
mail.sliit.lk - 216.239.36.21
mail.sliit.lk - 216.239.38.21
beta.sliit.lk - 143.204.225.115
beta.sliit.lk - 143.204.225.128
beta.sliit.lk - 143.204.225.38
beta.sliit.lk - 143.204.225.82
exchange.sliit.lk - 203.94.78.46
beta.sliit.lk - 2600:9000:2113:2200:7:ba06:4640:93a1
```

Next scan the Word Press using “wpscan”



```
kali@kali:~$ wpscan --url http://www.sliit.lk

WpScan
WordPress Security Scanner by the WPScan Team
Version 3.7.6
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://www.sliit.lk/
[+] Effective URL: https://www.sliit.lk/
[+] Started: Mon May 11 13:03:17 2020

Interesting Finding(s):

[+] https://www.sliit.lk/
Interesting Entries:
- server: nginx/1.10.3 (Ubuntu)
- via: 1.1 4a50ed5e34a0511ed5c53a2345c1f272.cloudfront.net (CloudFront)
- x-amz-cf-pop: CDG3-C1
- x-amz-cf-id: yP8tPm3f1rx8_X_VeBjxleFr8J6ZLmXboxS03W3Ylq6KjVI--sDLQ=
Found By: Headers (Passive Detection)
Confidence: 100%

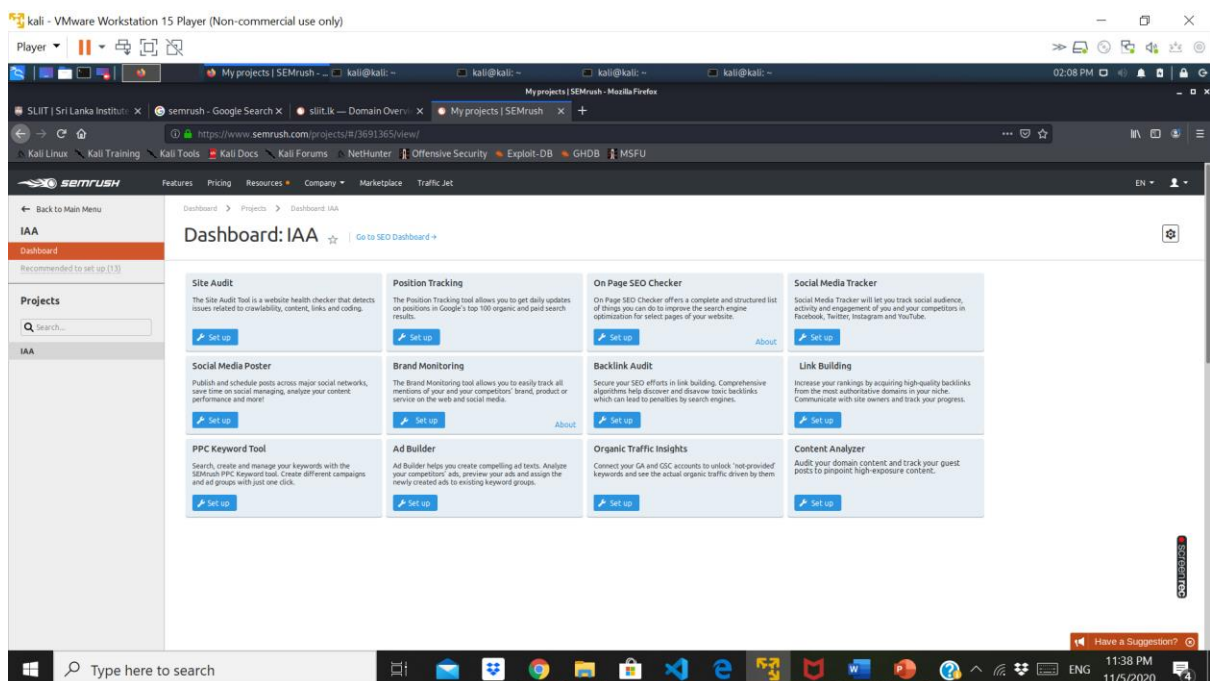
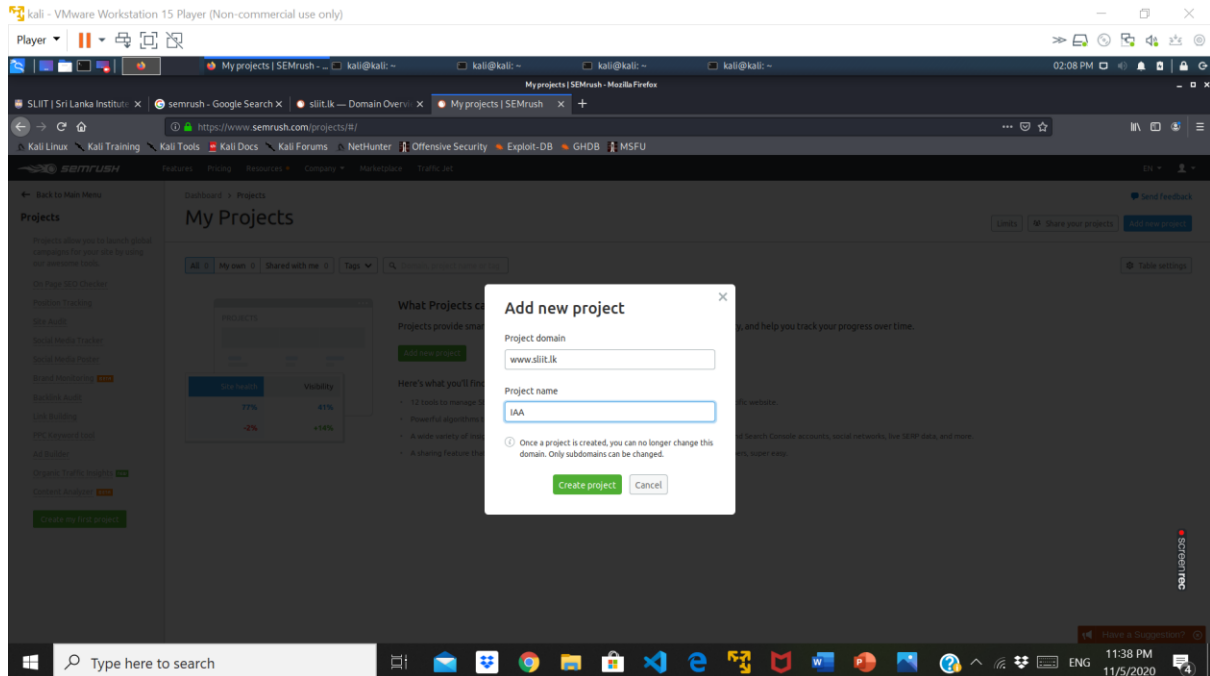
[+] http://www.sliit.lk/robots.txt
Found By: Robots Txt (Aggressive Detection)
Confidence: 100%
```

Next check if there is sql injection attacks.

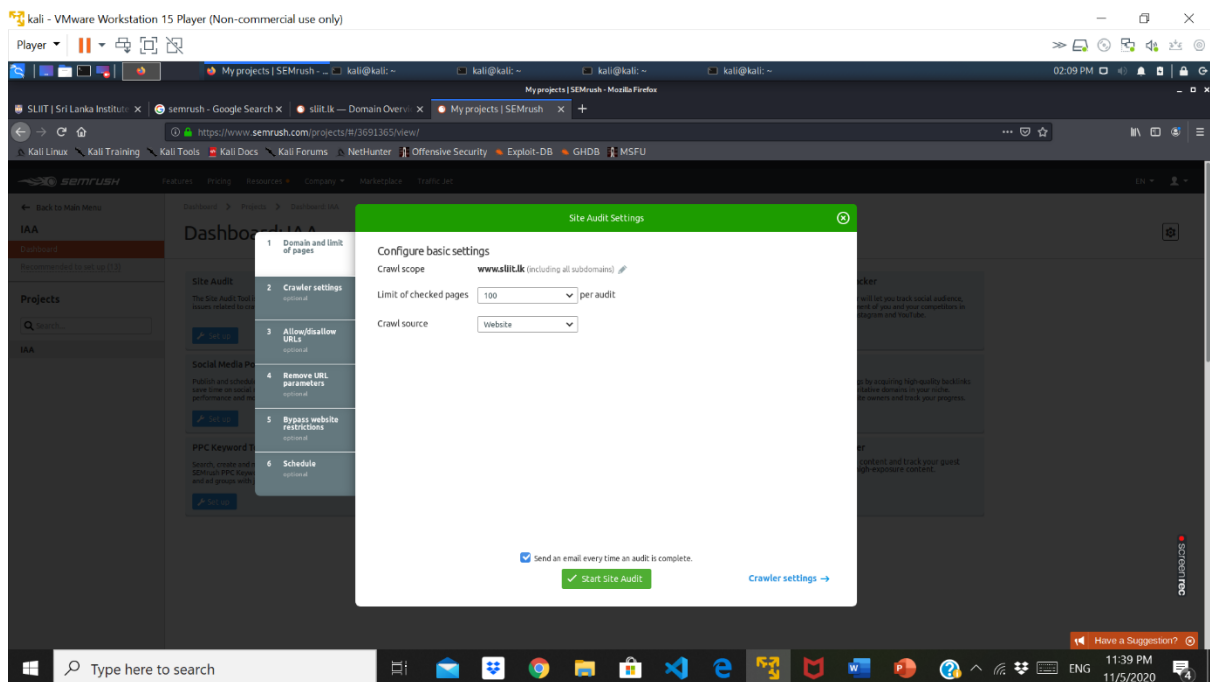
```
kali@kali:~$ sqlmap -u http://www.sliit.lk --dbs
kali@kali:~$ sqlmap -u http://www.sliit.lk --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal law
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 13:08:13 /2020-05-11/
[13:08:24] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.sliit.lk/'. Do you want to follow? [Y/n] Y
[13:09:04] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[13:09:04] [INFO] testing if the target URL content is stable
[13:09:10] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2
[*] ending @ 13:09:10 /2020-05-11/
kali@kali:~$
kali@kali:~$
```

Site-Performance checker using SEO (semrush tool)

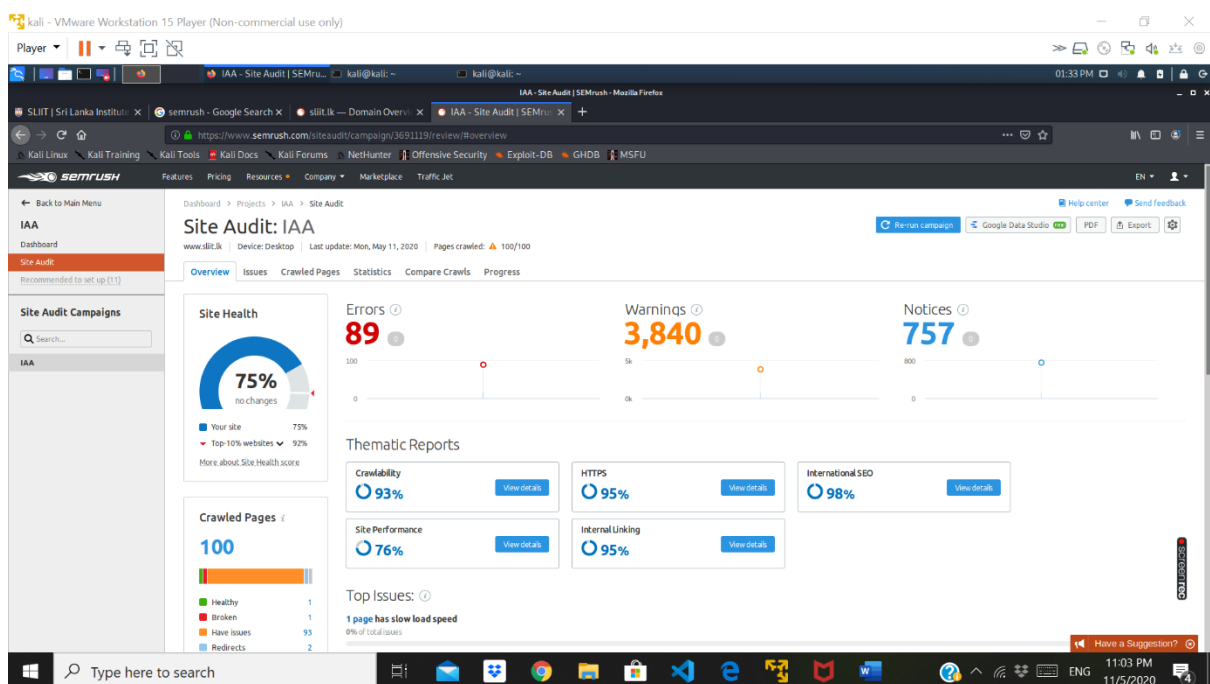
First, go to www.semrush.com and create an Account. Then you can create a new project and add your domain and project name.



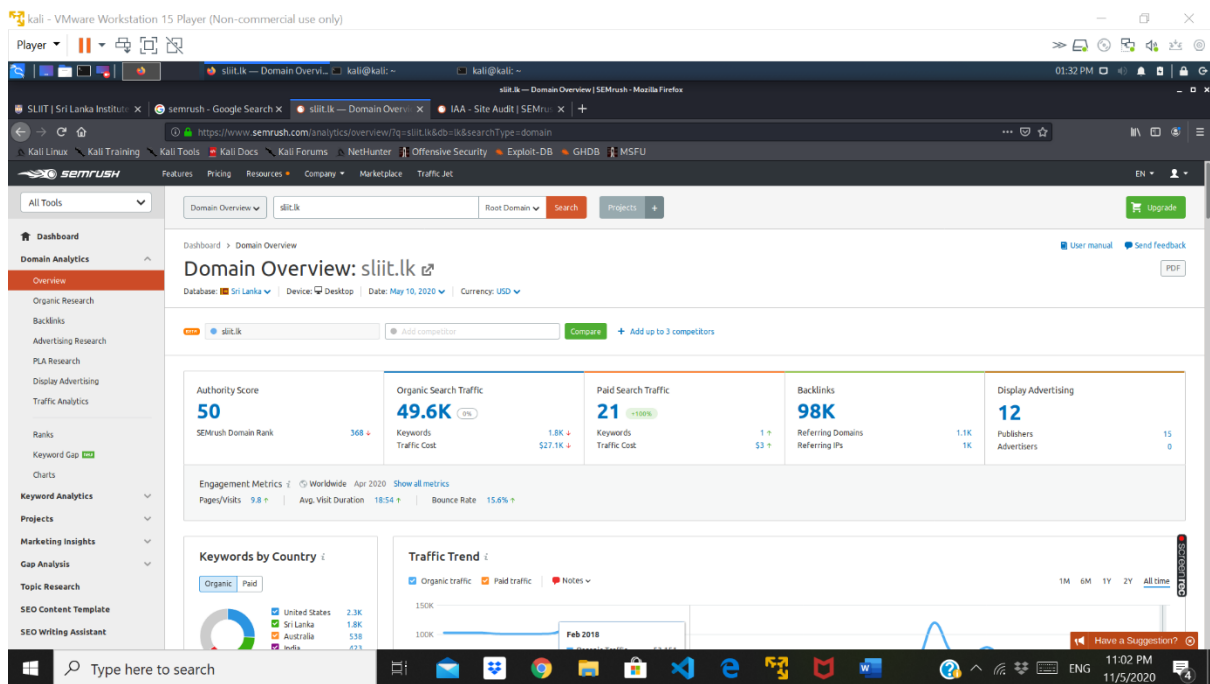
Then you can click on Site audit and start the audit.



Once it starts you can see the it with percentages levels and once your click on Site Audit you can view the test report.



From SEMrush tool you can do the Domain analytics by giving the Domain and the Country.



Problem Identification

This assessment was aimed to audit and penetrate SLIIT website. These security audits and penetration tests assist to improve the website security and the performance by eliminating the security vulnerabilities. The main vital fact is identifying what kind of security audit that the organization needs. Considering SLIIT institute, there are around 11000 students currently studying at SLIIT. It assists to guess large number of traffic arrive to SLIIT website. These facts proves that the security audit and penetrate testing should be conduct under several vital points.

- Can SLIIT website guarantee students' access credentials since SLIIT website has option
- redirect to course web?
- Does SLIIT webserver have high availability?
- Does SLIIT website is highly performance?
- Does SLIIT website highly optimized?
- Does SLIIT website have unpatched security issues?
- Does SLIIT website is securely hosted?
- Does SLIIT website open for any security attack?

The main identifications are listed above. SLIIT website is arrived large amount of traffic as mentioned above, therefore; it is vital to protect students private details. Current students can register, verify semester payments and many things through the SLIIT website moreover external users have to provide their personal details when they have to get some information, therefore; website must be secured properly. As a part of that having a up to date SSL certification is very important. The other main factor is having a highly performance and availability website to maintain a strong and reliable interactive between students and the institute. The other vital fact is to hosting on a well-known hosting provider. All these facts are the main problem dentifications of this assessment.

Recommendations

There are only few recommendations have to be performed since SLIIT website has a proper maintenance.

The SEO auditing proves that SLIIT website is well optimized. There are few recommendations that can be used to gain extra high SEO.

- Make permalinks including the keywords
- Remove unnecessary details that can slowdown the website such as large images, unnecessary plugins.
- Add keywords to images
- Update the website with recent plugins

The SQL injection test proves that SLIIT website is not vulnerable for a SQL injection but there were few HTTP errors could be found. The SEO auditing also proves there are few HTTP errors can be exploited by hackers, therefore; below show few recommendations.

- Managing website caching properly

The WPscan was performed since SLIIT website is a wordpress site according to the nmap outputs. The output proves that there are several outdated plugins are used in SLIIT website.

- Manage up to date plugins
- Remove unnecessary plugins that can slow down website performance

Several Nmap scanning showed many details about the SLIIT website such as open ports, ipaddresses, website hosting, and type of firewall, SSL certification and several staff members' names. SLIIT maintain proper security management for all of these mentioned points. The only vulnerability is few staff members' names because experienced hacker can guess email address of these users and send sphere phishing attacks including ransomwares. Below recommendation can mitigate those vulnerabilities.

- Implement DMARC authentication and reporting
- Train staff to recognize these attacks.
- Use multi-factor authentication

References

- [1] Inside Out Security. 2020. How To Use Nmap: Commands And Tutorial Guide | Varonis. [online] Available at: <<https://www.varonis.com/blog/nmap-commands/>> [Accessed 11 May 2020].
- [2] Blog.sucuri.net. 2020. [online] Available at: <<https://blog.sucuri.net/2015/12/using-wpsec-finding-wordpress-vulnerabilities.html>> [Accessed 11 May 2020].
- [3] Craig Campbell. 2020. Semrush Tutorial, Semrush Review, How To Use Semrush |. [online] Available at: <<https://www.craigcampbellseo.com/sem-rush-tutorial/>> [Accessed 11 May 2020].