

Arathon Technologies

Penetration Testing Report

27th October – 29th October 2020

Name: Lin Ligang Lincoln
Email Address: liligang@dso.org.sg
Report Date: 29th October 2020

Table of Contents

1. Summary	3
1.1. Objective	3
1.2. Requirements	3
1.3. Key Extractions	4
1.3.1. Credentials	4
1.3.2. Network Map	4
2. Web Server (54.237.125.183).....	5
2.1. Enumeration	5
2.1.1. Nmap.....	5
2.1.2. WPScan	10
2.1.3. Information Gathering	11
2.2. Exploitation.....	13
2.2.1. InfiniteWP Plugin	13
3. Bastion Host (18.210.159.19/10.0.2.5)	14
3.1. Nmap	14
3.2. Ping Sweep	21
4. KennyYap Client Machine (10.0.0.5).....	22
4.1. RDP Access	22
4.2. Nslookup.....	22
4.3. Observations	24
5. Domain Controller (10.0.1.10)	25
6. File Server (10.0.1.11)	30
6.1. Observations	30
7. Additional Observations	32
7.1. Firewall Setup	32
8. Logs	33

1. Summary

1.1. Objective

Our honeynet is emulating a Windows Domain network, the point of entry is an internet-facing web server. The PT objectives are:

- (1) map the Windows network, including Windows user account.
- (2) get Domain admin credentials.

You only need an internet facing machine. The usual kali/metasploit set of tools will be sufficient. I will give you the webserver URL next Tuesday 27 Oct 2020 and check in with you at the end of each day of the exercise. The exercise will be 27 - 28 Oct 2020. We can have a debrief on Fri 30 Oct.

Your participation will help us validate our sensors in the honeynet. As you navigate through the system, can you keep a log of your actions (timestamps, screenshots and short description in point-form is enough). This can help us validate your actions against what the sensors are capturing. We keep things simple, no need for formal report. At the end of the exercise, you can submit the logs with a summary of findings. We will use this information to validate the sensors so pls include timestamps to each set of activity you did.

1.2. Requirements

The following was carried out to fulfil the objective

1. Obtaining credentials from the Web Server to enter internal network
2. Enumeration of domain users and computers
3. Plotting out the network map of the organization
4. Contents available in Windows Clients

1.3. Key Extractions

1.3.1. Credentials

The following table shows the credentials that were obtained with the source mentioned

Credentials	Source	Value
Bastion Host (18.210.169.19/10.0.2.5)	Given	User: sshtun Pass: dso2020
KennyYap AD User	Given	User: ArathonDomain\kennyyap Pass: Sam0129200!my

1.3.2. Network Map

This is the network map that could be mapped after enumeration and information dump retrieval. More information about what they are in the report and logs

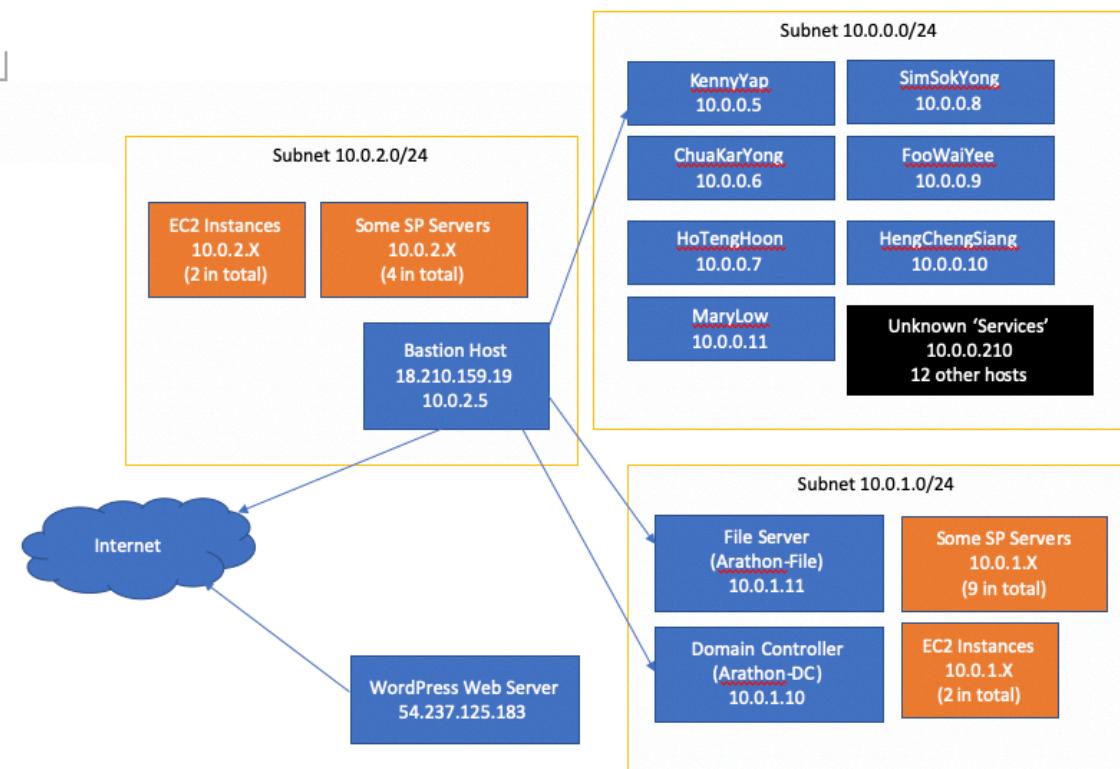


Figure 1: Network Map

2. Web Server (54.237.125.183)

2.1. Enumeration

2.1.1. Nmap

Did three forms of scans for resource efficient purposes

1. Did an initial scan for the Top 50 TCP ports used by the Web server
2. Did a full scan after the initial scan
3. Did a UDP scan in case UDP is used by the server

```
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
```

Figure 2: Initial Scan

```
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.  abouts 50 --open -oA nmap/initial 54.237.125.183
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.nse/initial.nmap for writing
Initiating NSE at 21:51
Completed NSE at 21:51, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.nse      jsfiles.py      li2u-output      Music
Initiating NSE at 21:51      gitleaks-linux-amd64.jsfiles.sh      linkedin2username-master      nmap_1
Completed NSE at 21:51, 0.00s elapsed payload.py      lab-connection      mssqlclient.py      OSCP.c
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 21:51--sv=0 --top-ports 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 21:5137-125-183.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 (use 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
SYN Stealth Scan Timing: About 3.87% done; ETC: 22:04 (0:12:51 remaining) ::/0/microsoft:windows_xp:ps
SYN Stealth Scan Timing: About 5.74% done; ETC: 22:08 (0:16:42 remaining) * 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) 54.237.125.183) are open|filtered
SYN Stealth Scan Timing: About 69.67% done; ETC: 22:24 (0:10:14 remaining)
SYN Stealth Scan Timing: About 74.29% done; ETC: 22:24 (0:08:21 remaining)
SYN Stealth Scan Timing: About 78.92% done; ETC: 22:24 (0:06:28 remaining)
SYN Stealth Scan Timing: About 83.55% done; ETC: 22:24 (0:04:35 remaining)
SYN Stealth Scan Timing: About 88.18% done; ETC: 22:24 (0:02:42 remaining)
SYN Stealth Scan Timing: About 92.81% done; ETC: 22:24 (0:01:49 remaining)
SYN Stealth Scan Timing: About 97.44% done; ETC: 22:24 (0:00:56 remaining)
SYN Stealth Scan Timing: About 100.00% done; ETC: 22:24 (0:00:54 remaining)
```

```
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. 0 ports | open -oA nmap/initial 54.237.125.183
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.nmap/initial.nmap for writing
Initiating NSE at 21:51
Completed NSE at 21:51, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.loads      jafiles.py      libnmap-output      Music
Initiating NSE at 21:51      ditileaks-linux-amd64  jisfiles.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 -O --top-ports 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 37-125-183.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-rate-limit
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 method 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 use 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 [2012]
SYN Stealth Scan Timing: About 3.87% done; ETC: 22:04 (0:12:51 remaining) ::/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) 5.183 )
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) 237.125.183 ) are open|filter
SYN Stealth Scan Timing: About 69.67% done; ETC: 22:24 (0:10:14 remaining)
SYN Stealth Scan Timing: About 73.10% done; ETC: 22:23 (0:08:24 remaining)
SYN Stealth Scan Timing: About 76.53% done; ETC: 22:22 (0:07:34 remaining)
SYN Stealth Scan Timing: About 80.00% done; ETC: 22:21 (0:06:44 remaining)
SYN Stealth Scan Timing: About 83.43% done; ETC: 22:20 (0:05:54 remaining)
SYN Stealth Scan Timing: About 86.86% done; ETC: 22:19 (0:04:54 remaining)
SYN Stealth Scan Timing: About 90.29% done; ETC: 22:18 (0:03:54 remaining)
SYN Stealth Scan Timing: About 93.72% done; ETC: 22:17 (0:02:54 remaining)
SYN Stealth Scan Timing: About 97.15% done; ETC: 22:16 (0:01:54 remaining)
SYN Stealth Scan Timing: About 100.00% done; ETC: 22:15 (0:00:54 remaining)
```

```

|_ 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: 0d7d32 59db 27a1 6a59 125d 04a1 af86 c312
|_ SHA-1: cfda b5ea 0912 2140 2bf7 02c9 0bc8 0729 83e6 7c8f
|_ -----BEGIN CERTIFICATE-----
MIIF7zCCBNegAwIBAgISA9vgoQPgGSIJCjdUQKg+rVz11MA0GCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTAjVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MSMwIjQYDVQQD
237.125.183
ExpMZXQncyBFbmNyeXB0IEF1dGhvcmloesBYMzAeFw0yMDA5MjMwNzEzMjJaFw0y
MDEyMjIwNzEzMjJaMYxJDAiBgNVBAMTG3d3dy5hcmF0aG9udGVjaG5vbG9naWVz
LmNvbTCCAAIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGBAJeML1yxqisQLwkO
l 54.237.125.183
9gwkFAax8Yb0dpEtS/hEdeSTCPToOB2ZHkuvtfVOCAVXrooOk+LumNA3G7mbQCb2
57/XgJQzrKgmIEiaWmd5xSJ5cwwE3jegXcncc1ztfcf7WU0ke7N5akn6mYWdSR4P
z0dQZ5wwz8nEV7l+vp2yZ2I3Jx9UH8rwxSUI2E8juB3ID4I9zDjPWBY2h43lf7J
sE8o7kYpygMBaYzz4As8zoBkc/Cy2Gr1WDHTbp7YsCUSJ4mOM3zvnHxlvapU9N0V
WeaCo0I0w7z0/YaDAGJvNRcDXWJLxrLQxA6VEJtkqGwGl/DNa5KaVbfVHZLDs6F
L8quDmtwqkFtwz3fgPDqTwpc8fr8CbvrTn70uzXbj+84mTXiTkoXAN2p70kHIM2a
5Dz0vQ3cwf7sAgl7kuGwB/+bCGK019zwxgN1F7KocB4oNTKTNoWMATKF2r0pWP7F
j8alyAonQvowGE2XLXAnij7t6Wqy6tgNVKkFmW7dvo0f42CsVwIDAQABo4ICcTCC
Am0wDgYDVR0PAQH/BAQDAGWgMB0GA1UdJQ0WMBQGCCsGAQUFBwMBBgrBgfFBQcD
AjAMBgNVHRMBAf8EAjAAAMB0GA1UdDgQWBBTnIBnHoDtSDNsWk3Tz5tlpif3wjAf
BgNVHSMEGDAwgsOmpjBH3duubR0bemRWXv86jsotBvBgggrBgfFBQcBAQRjMGew
LgYIKwYBBQUTHMAGGImh0dHA6LyvY3NwLmludC14My5sZXrzzW5jcnlwcd5vcmcw
LwYIKwYBBQUTHMAKG12h0dHA6Ly9jZXJ0LmludC14My5sZXrzzW5jcnlwcd5vcmcv
MCYGA1UdEQQfMB2CG3d3dy5hcmF0aG9udGvjaG5vbG9naWVzLmNvbTBMBgNVHSAE
RTBDMagBmeBDAECATA3BgsrBgEEAYLfEwEBATAoMCYGCCsGAQUFBwIBFhpodHRw
O18vY3BzLmxldHNlbmNyeXB0Lm9yZzCCAQUGCCsGAQQB1nkCBAIEgfYEGfMA8QB2
APCVpFnyANGCQBAtL50Ijq1L/h1H45nh0DSmsKiqjrJzAAABdLoGMewAAAQDAEcw
RQIgOXCVYRI8x4LQJIn0g4BGdgY/HNMnixuVzmVTLD818YCIQCScsVzls4woT5WJ
Xpogae88qpBcGH5Fq+reYuL5+lb6SQB3ALIEBcyLos2KIE6HzvkruYolIGdr2vpw
57JJUy3vi5BeAAABdLoGMeoAAQDAEgwRgIhAKQweUuMCKk+cFDx8I3dyIpH+r6l
6cQ/0kcLwmwti7DxAiEAonKbFrWXmSZTs5XgFznba+CZ6yBmyukOn//SVlWagkw
DQYJKoZIhvcNAQELBQADggEBADJ0tuBLbEfLeCmHghJ6wIg0jJWWzaD8g7ku5j2G
zD0rnsYhXXsZt4m0mj28xeLTIn7cvVmUBSMizkdzRj52w77unFi41zYWW+Mn3
UdtXR7eX5DMPfqH+/Gav4U6BEtS3HjfVOX5ZddERucWf6IC1cB7ENwIeMh8aFXJ
JdlHPV0xcMMPV36iztzqShB7i8RgNLRzjgrz6knr95QcNBnu20PE3+dwCGFrOdzm/
FrUoOzjrP3qiBHyqlQ5kzAN/46V5JV9PLwH92HN19Kyf3ZeRapiPB9WzgGhSdUUm
EYxJrrlxdtT7UGJ8YDeajKmyuL4m1RpstMuA0pIAUOWi4= 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- -oA 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-1EK502L5-183.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 deb7e5
-----BEGIN CERTIFICATE-----
MIIC4jCCAcgAwIBAgIQL8xiBuWt6FEEnWPOYHAp1DANBgqhkiG9w0BAQsFADAA
MRgwFgYDVQQDEw9FQzJBTUFaLTFFSzUwMkwwHhcNMjAwODI0MTI0MzA2WhcNMjEw
MjIzMjMTI0MzA2WjAaMRgwFgYDVQQDEw9FQzJBTUFaLTFFSzUwMkwwggEiMA0GCSqG
SIB3DQEBAQAA4IBDwAwgEKAOIBAC7ny1mAhh773Wg5gPjPn9sPPd3cDyu5q25
Y33sDEYF0nD/hHCJGtbYrZJk0rXuv89qBj5A8jxh0Tt8/Yf2sQ/uQnH2TEuyB05
KdInsp9kPUOegwQX70pFX9+INRH++AJcurIQZ+cb9QkXWewQt+kigABMae8NX3iH
A+fsQbrEBveCik1U38zVdeV8SzypMPaZ+nzNtEP65wSErcenDff77l1WvP1pEM
W/b13evT6+JEtb0ooC6HAHPIxUCsEVfsJXO+e4D4ttIfJv3nQnGywT/DCc64nlAr
ayqLBhlepUDxInB4lw3ra926l10ZTRTzvuuCcx2A1gQHBFREbMVAgMBAAGjJDai
MBMGA1udJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAWIEMDANBgqhkiG9w0BAQsF
AAOCQAQEBKdkrn+FjytAG01D6aV3mY4QEePNcsk2LbzzzTcaHsFA9zLW0o9PGgZ
xwF2ixW2WSX/Drge1QPzk1Bg2W2a+pAAVGh22ujklTq832U3C7wjgut9cBRiwX6V
d9/CYhfA42NsvdkyHyhfmNbTz3YM6kvhVQDCF13klnnQMFaDmwGKuppcc0dtPftN
Njs0xgCxbBgcwOKKfx/StlJBjeo2QqVUnfhf5tdwvKrsgeh8/EJdcX5P0jKcmq
204dxBNLY/eZqAF0zQAZ/GoyqruoW5pQj9bBDFm2nLjKIUGjVU+7GOj40KghpcG
PIee23sgHVQ4QicwrgVXV7tpJJM8A=-----END CERTIFICATE-----Microsoft IIS httpd 10.0
_ssl-date: 2020-10-27T02:22:47+00:00; +13s from scanner time./UPnP)
Warning: OScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose (unreliable because we could not find at least 1 open and 1 closed port)
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) | cpe:/o:linux:linux_kernel:3.2 | cpe:/o:microsoft:windows_xp::sp3
TCP/IP fingerprint: (Windows 7, Windows 7, Linux 3.2, Microsoft Windows XP SP3, Microsoft Windows XP SP2)
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:inux-gnu)SEQ(SP=F2%GCD=1%ISR=10B%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=O%A=S+F=AS%R
OS:D=0%Q=)T2(R=N)T3(R=Y%DF=N%TG=80%W=FAF0%S=O%A=S+F=AS%O=M5B4%RD=0%Q=)T4(R
OS:=Y%DF=N%TG=80%W=7FFF%S=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)
-----END NMAP REPORT-----$ 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 (5.232MB)

```

Figure 3: Full Scan

```

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 1735.60 seconds (5.232MB)

```

Figure 4: UDP Scan

Based on the results of the scan, we can determine the following information:

- Ports 80 (HTTP), 443 (HTTPS), 3389 (Microsoft RDP) are open
- Can observe that the webserver is running on Amazon AWS EC2
- Can determine that Microsoft IIS server is managing the front end webpage
- Computer name is EC2AMAZ-1EK502L
- Product Version is 10.0.17763, meaning it is a Windows Server 2019
- SSL- cert retrieved on both port 443 and 3389 -- Shows SSL is enabled

2.1.2. WPScan

Triggered a default WPScan on the Target

```
[+] Do you want to update now? [y/n]: n[INFO] detected: iinfo
[+] URL: https://www.arathontechnologies.com/ [54.237.125.183]
[+] Started: Mon Oct 26 22:05:38 2020
[+] Finished: Mon Oct 26 22:05:48 2020
Interesting Finding(s):
[+] Headers with %20
  Interesting Entries:
    - server: Microsoft-IIS/10.0
    - x-powered-by: PHP/7.4.9
  Found By: Headers (Passive Detection)
  Confidence: 100%
[+] XML-RPC seems to be enabled: https://www.arathontechnologies.com/xmlrpc.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100% (for OS scan) requires root privileges.
  References:
    - http://codex.wordpress.org/XML-RPC_Pingback_API
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
    - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
    - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
[+] https://www.arathontechnologies.com/readme.html
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%
[+] This site has 'Must Use Plugins': https://www.arathontechnologies.com/wp-content/mu-plugins/
  Found By: Direct Access (Aggressive Detection)
  Confidence: 80%
  Reference: http://codex.wordpress.org/Must_Use_Plugins
[+] The external WP-Cron seems to be enabled: https://www.arathontechnologies.com/wp-cron.php
  Found By: Direct Access (Aggressive Detection)
  Confidence: 60%
  References:
    - https://wp-cron-server.MSFT.ms Microsoft Terminal Services
      - https://www.iplocation.net/defend-wordpress-from-ddos
      - https://github.com/wpscanteam/wpscan/issues/1299
[+] WordPress version 4.8.14 identified (Latest, released on 2020-06-10).e:/o:microsoft:windows_xp:tsn3_cnet/o:microsoft:window
  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
```

Figure 5: WPScan

This is what we can understand based on the scan results:

- 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 for 4.8 series)
- Theme is twentyseventeen (OOB version)
- No plugins are used but "Must-Use Plugins" are available

Had limited knowledge on what "Must-Use Plugins" (mu-plugins) so did not explore on that.

2.1.3. Information Gathering

The "Home" Page link on the website placed the IP Address (54.237.125.183) of the Web Server

There is a misconfiguration in the Web Server which caused an private post to be shown publicly

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.

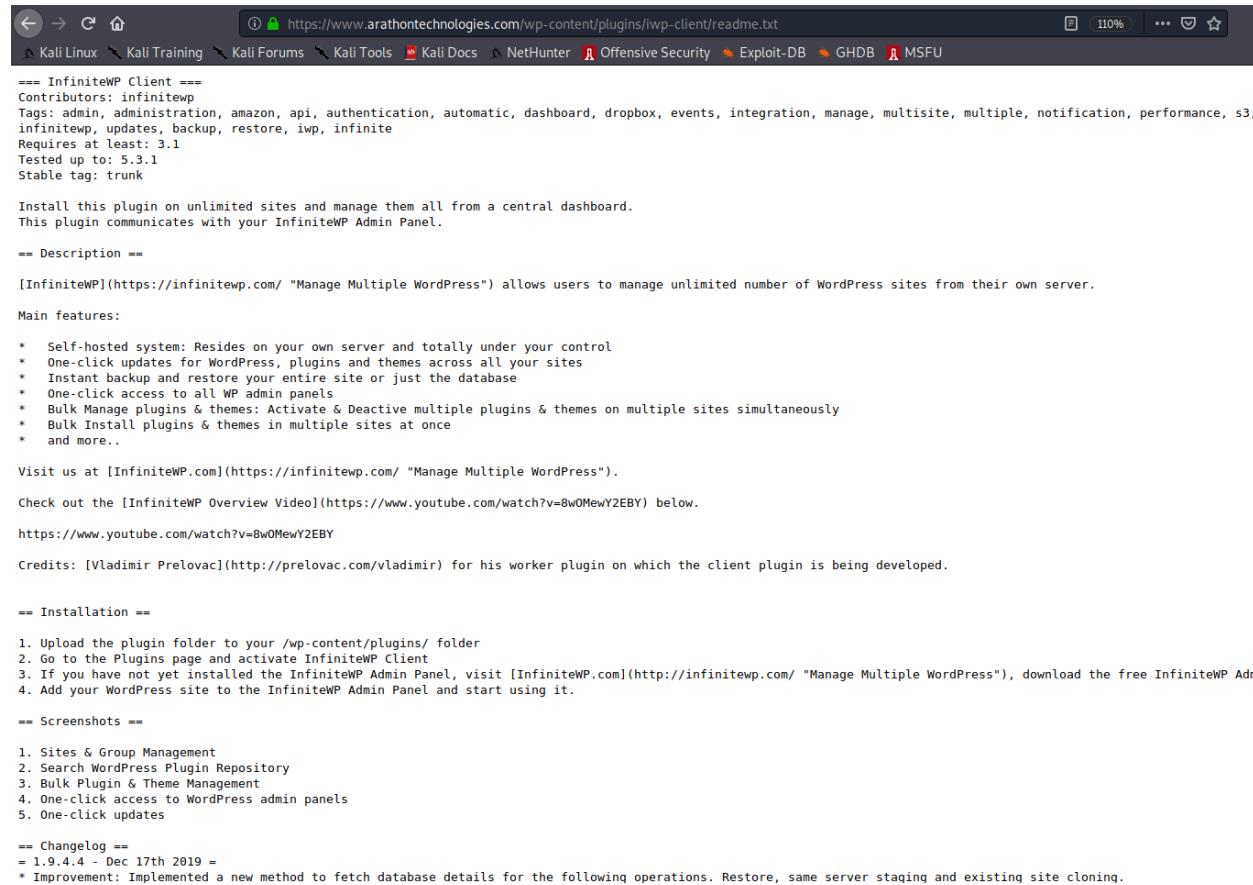
Thanks.

KennyYap

Figure 6: Unprivatized Post

The post mentioned of using a common username like “wordpress” for their login credential, as well as a mention that the plugin “InfiniteWP” is used.

The WPScan did not capture that the plugin is used, so I had to manually check that the plugin is there by looking for the readme file.



A screenshot of a web browser window displaying the README.txt file for the InfiniteWP Client plugin. The URL in the address bar is <https://www.arathontechnologies.com/wp-content/plugins/iwp-client/readme.txt>. The page content includes the plugin's license, description, features, installation instructions, screenshots, and changelog. Key sections include:

- == InfiniteWP Client ==**
- Contributors:** infinitewp
- Tags:** admin, administration, amazon, api, authentication, automatic, dashboard, dropbox, events, integration, manage, multisite, multiple, notification, performance, s3, infinitewp, updates, backup, restore, iwp, infinite
- Requires at least:** 3.1
- Tested up to:** 5.3.1
- Stable tag:** trunk
- 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 & Deactivate multiple plugins & themes on multiple sites simultaneously
 - * Bulk Install plugins & themes in multiple sites at once
 - * and more..
- 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
 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:**
 - = 1.9.4.4 - Dec 17th 2019 =
 - * Improvement: Implemented a new method to fetch database details for the following operations. Restore, same server staging and existing site cloning.

Figure 7: InfiniteWP Readme File

In it, I noted down that the version of the Plugin is 1.9.4.4.

Lastly, I did a user enumeration by using a Wordpress “author” vulnerability that comes with default templates and configuration.

Using it, I obtained the following information.

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

2.2. Exploitation

2.2.1. InfiniteWP Plugin

Searching on Exploit-DB for any exploits on the plugin, I managed to find two exploits: One using Metasploit, while one using Python.

The screenshot shows the Exploit Database Advanced Search interface. The search parameters are set to "Title: InfiniteWP", "CVE: 2020-1234", and "Type: Exploit". The results table displays two entries:

Date	Type	Title	Platform	Author
2020-02-11	webapps	WordPress Plugin InfiniteWP - Client Authentication Bypass (Metasploit)	PHP	Metasploit
2020-01-17	webapps	WordPress Plugin InfiniteWP Client 1.9.4.5 - Authentication Bypass	PHP	Raphael Karger

Figure 8: Exploit-DB Results on InfiniteWP

Being more familiar with Python, I tried that one first using the username as “wordpress” since that is already provided by the private post.

However, I was not able to trigger any successful unauthenticated bypass into the backend.

Repeated the attempts with the different usernames, thinking there might be some form of privilege level being assigned to the different users involved. However I am unable to get a successful bypass.

Tried to use the Metasploit to try to achieve the same goal. But it was unsuccessful as well.

3. Bastion Host (18.210.159.19/10.0.2.5)

As my bypass was not successful, I requested for the credentials to be provided to me to carry on the exercise. This was what was provided to me.

Deliberate traces left on web server machine to lead attacker to Arathon network:

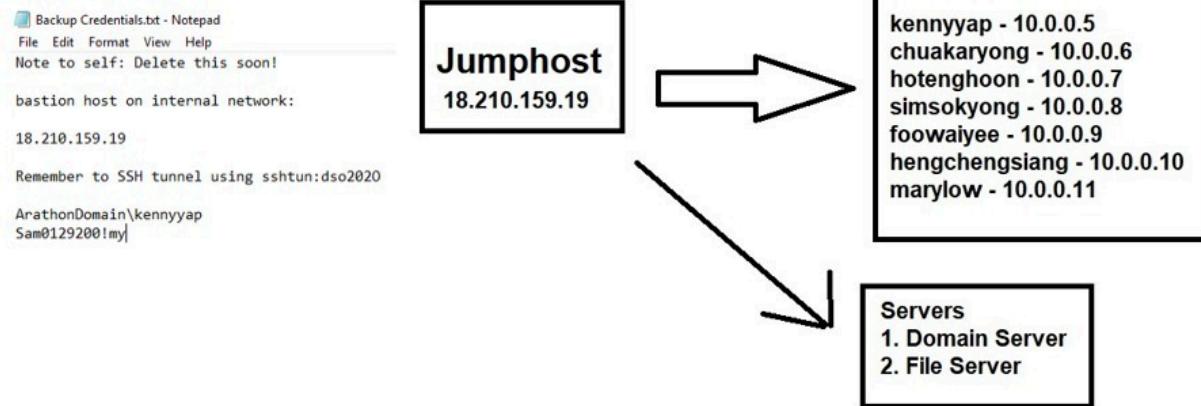


Figure 9: Credentials Given to me

Based on this information, I know that there is a Bastion Host to connect to in order to enter the internal network, and SSH credentials that I could use to enter it. I am also provided with the user credentials of kennyyap which I could test later when I successfully enter the domain.

3.1. Nmap

Thinking that I was not provided with the network map shown above, I decided to do a proper enumeration scan on the network. As the bastion host was on the subnet 10.0.2.0/24, I decided to first do a ping sweep scan on the subnet (Command: **nmap -v -sn 10.0.2.1-254 -oG ping-sweep.txt; grep Up ping-sweep.txt | cut -d " " -f 2**). However, the only result I obtained in the scan was the bastion host is up. I then did a decrement on the network subnets to see what results I would get. I eventually get this list of IPs that are up (excluding the bastion host)

1. 10.0.0.4
2. 10.0.0.25
3. 10.0.0.45
4. 10.0.0.66
5. 10.0.0.73
6. 10.0.0.84
7. 10.0.0.115
8. 10.0.0.117
9. 10.0.0.132
10. 10.0.0.197
11. 10.0.0.206
12. 10.0.0.210
13. 10.0.0.222
14. 10.0.1.11

```
Nmap done: 254 IP addresses (13 hosts up) scanned in 2.23 seconds
10.0.0.4  Library(scanner/http/wordpress_xmlrpc_login) > set SSL true
10.0.0.25  Aborting the SSL option's value may require changing REPORT!
10.0.0.45  Aborting
10.0.0.66  Library(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)
10.0.0.132  my module execution completed
10.0.0.197  Library(scanner/http/wordpress_xmlrpc_login) > exit
10.0.0.206  $ sudo nc -nlvp 4444
10.0.0.210  word for kali:
10.0.0.222  in [any] 4444 ...
```

Figure 10: Nmap scan results for 10.0.0.0/24 subnet

Finding it odd since I cannot enumerate the “users’ machines” that I was expecting to, I decided to try to detect them through an initial scan on the top 50 TCP ports.

```
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).
  .Lrcp.php - Sending Hello...
  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:6.0
  .Sudo nc -nlvp 4444
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
root@kali:~#
```

Figure 11: Initial scan on Subnet 10.0.0.0/24

I did not find any result, but only that the IP 10.0.0.210 has a OpenSSH service available to ssh into, which I did not do so. I then shifted my attention to try to do a manual ping to see if the machine are alive.

While that was happening, I ran a full scan on all the machines that I have found to be up (Command: `nmap -sC -sV --open -p- -oA full -vvv -iL pingsweep.txt`).

```
Completed NSE at 09:51, 0.00s elapsed 73.200:4444/tcp
Initiating Ping Scan at 09:51
Scanning 14 hosts [2 ports/host] (sable_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
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
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
NSE: Script scanning 4 hosts. at http://54.237.125.183/wp-login.php
NSE: Starting runlevel 1 (of 2) scan. --access: Could not obtain cookie for wordpress
Initiating NSE at 09:52 but no session was created.
Completed NSE at 09:52, 0.03s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 09:52/unix/webapp/wp_infinitewp_auth_bypass:
Completed NSE at 09:52, 0.01s elapsed
Initiating Connect Scan at 09:52
Scanning 10 hosts [65535 ports/host]
Discovered open port 445/tcp on 10.0.1.11
Discovered open port 80/tcp on 10.0.1.11
Discovered open port 139/tcp on 10.0.1.11
Discovered open port 22/tcp on 10.0.0.210
Discovered open port 443/tcp on 10.0.1.11
Discovered open port 3389/tcp on 10.0.1.11
Discovered open port 135/tcp on 10.0.1.11
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)
```

```

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 REPORT!
Completed Connect Scan at 10:21, 1702.18s elapsed (655350 total ports)
Initiating Service scan at 10:21 (temp with ignored) > check
Scanning 11 services on 10 hosts reliably check exploitability. Is the site online and running?

```

```

Initiating Service scan at 10:21
Scanning 11 services on 10 hosts
Completed Service scan at 10:21, 53.58s elapsed (11 services on 10 hosts)
NSE: Script scanning 10 hosts.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:21
NSE Timing: About 99.48s done; ETC: 10:22 (0:00:00 remaining)
NSE Timing: About 99.61s done; ETC: 10:23 (0:00:00 remaining)
NSE Timing: About 99.74s done; ETC: 10:23 (0:00:00 remaining)
Completed NSE at 10:23, 90.79s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.07s elapsed
Nmap scan report for 10.0.0.210
Host is up, received comm-refused (0.0041s latency).
Scanned at 2020-10-28 09:51:32 +08 for 1918s
Not shown: 65534 filtered ports
Reason: 65534 conn-refused
PORT      STATE SERVICE REASON VERSION
22/tcp    open  ssh   syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 7e:87:9b:92:2e:7d:c9:09:dc:d0:97:ac:a6:0b:7f:be (RSA)
| ssh-rsa AAAQABJQKvC1cZEMzDADoA0BAAQACQWNEc6x0p2A...Nhnv/pE15dy0ed+uArVzKkyUxVZ+bIkNZ01r30P7TLF/B8XUHYD1HXPu...02w0b4+llyO20jrYW...5hFrwybxsgJY...02w4F9GkQJNW+j18PEgJ6hByCTs+ZrVJpKG
NSE: Script scanning 10 hosts
NSE: Starting runlevel 2 (of 2) scan.
Completed NSE at 10:23, 2.08s elapsed
NSE Timing: About 76.62s done; ETC: 10:24 (0:00:00 remaining)
NSE Timing: About 76.75s done; ETC: 10:24 (0:00:00 remaining)
Completed NSE at 10:24, 90.79s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:24
Completed NSE at 10:24, 0.07s elapsed
Nmap scan report for 10.0.0.1.11
Host is up, received syn-ack (0.0005s latency).
Scanned at 2020-10-28 09:51:32 +08 for 1918s
Not shown: 65525 filtered ports
Reason: 65525 no-responses
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON VERSION
80/tcp    open  http        syn-ack Microsoft IIS httpd 10.0
| http-auth:
|_ HTTP/1.1 401 Unauthorized\r\n
| Digest algorithm=MD5-sess nonce=+Upgraded+vlefd4f7231ea1da7003fe8af21c717f3cc72ac11dd1acd60170265652e485fd1bc2c76368899f7e2d016eb46a7f6c85f8d4b6743b6de1fcfa charset=utf-8 qop=auth realm=Digest
| Negotiate
|_ NTLM
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

```

[+] NTLM
http-ntlm-info: 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 stain cookie for wordpress
DNS_Tree_Name: ArathonDomain.internal created.
Product_Version: 10.0.14393
http-server-header: Microsoft-IIS/10.0
http-title: Site doesn't have a title.(infinityauth_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 IN 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.internal CIDR identifier, or hosts F
Issuer: commonName=ARATHON-FILE.ArathonDomain.internal (TCP)
Public Key type: rsa no Negotiate SSL/TLS for outgoing connections
Public Key bits: 2048 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
SHA1: 4e10 0016 b67c 5d35 5ad4 c2c1e067 3ae0 5f90 3fb7
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIQOZWyLiG5MYNI36Del+Z/XzANBgkqhkiG9w0BAQsFADu
MSwwKgYDVQDDeNBukFUSE90LUZJTEUoQXJhdGhbkrVbWFpbis5pbnRlcmb5hbDAe
Fw0yMDA5MjIwMjI5NDdaFw0yMTAzMjQwMjI5NDdaMC4xLDAqBgvNBAMTI0FSQVRI
-----END CERTIFICATE-----
T04trKlMRS5BcmF0aG9uRG9tYWluLmludGVybmsMIIBIjANBgkqhkiG9w0BAQE
AAOCAQ8AMIIIBCgKCAQEAs5nlBcRbCnSeWieD8c4RxFQBGAWCkemnhzOZvru6BWIj
Bd4Le04ZMcBBDHcpvItkQIPcMWQw9K6HONO/wcJ3YKRrKXDwqE38CjY00sbpsbK
ApAYrTg2uergTpc486jMeEST+0FI/dl4eKftH1Mb5Q/9RtGztqUWPrIbv7W97jTU
PXbkmvCJcXltIyh7Sw9p9rstk0JanvOf/q9RsB+JPU6K3uZLAi7dMuim8Z4WL8/
caQX7jvGfcQe9uRM0juLsWePp3YRxUCghcZlwFAHiEf6vIeJ5kh5+0g5FGXG0UY8
cpywQi/ThR2URge5ozRf59pQLJ6XP1df48CbicT2DQIDAQABoyQwIjATBgNVHSUE
DDAKBngrBgfFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvNAQELBQAQggEBAXxs
5PlNf7Td+zZ6HuHXonbqKeCYY5HJvmPGDqkeM8J2QN+kzKtUa9XANWkeCkATED3l
xsDMUK9guK1RmvQ2gpUmZb9EsOVTME8MOBNi0GBo30qtDdCinCDhr6aXZfkI25U6
1Ttdd70IqlqxPwyfh1r9nC8kwYLT2jPZ0g00e41VQ7PRmcQDZ25hRbaBUnyQlaK0
8DNdZgWEYtMVPYB3EhlDmpVr6p/JQZPlYl7W3Jd6eOMDc9Xc1Ef7i5+6vWZDI3Ro
UCgRbHo5qVFsn0nHQWSkxkl70s40l+4ITHWc3waFgIs4DUTp8fi3Ax3VgmPmtfMDI
02/jxIFT0sj6GaCV8yU=
-----END CERTIFICATE-----
http-ntlm-info: to bind to 138.75.173.200:4444; - -
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 (bypass) > check
http-title: Not Found - Cannot reliably check exploitability. Is the site online and running Wo
5986/tcp open ssl http/2 syn-ack Microsoft SChannel TLS

```

```

[+] NTLM
http-ntlm-info: 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 stain cookie for wordpress
DNS_Tree_Name: ArathonDomain.internal created.
Product_Version: 10.0.14393
http-server-header: Microsoft-IIS/10.0
http-title: Site doesn't have a title.(infinityauth_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 IN 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.internal CIDR identifier, or hosts F
Issuer: commonName=ARATHON-FILE.ArathonDomain.internal (TCP)
Public Key type: rsa no Negotiate SSL/TLS for outgoing connections
Public Key bits: 2048 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
SHA1: 4e10 0016 b67c 5d35 5ad4 c2c1e067 3ae0 5f90 3fb7
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIQOZWyLiG5MYNI36Del+Z/XzANBgkqhkiG9w0BAQsFADu
MSwwKgYDVQDDeNBukFUSE90LUZJTEUoQXJhdGhbkrVbWFpbis5pbnRlcmb5hbDAe
Fw0yMDA5MjIwMjI5NDdaFw0yMTAzMjQwMjI5NDdaMC4xLDAqBgNVBAMTI0FSQVRI
-----END CERTIFICATE-----
T04trKlMRS5BcmF0aG9uRG9tYWluLmludGVybmsMIIBIjANBgkqhkiG9w0BAQE
AAOCAQ8AMIIIBCgKCAQEAs5nlBcRbCnSeWieD8c4RxFQBGAWCkemnhzOZvru6BWIj
Bd4Le04ZMcbBdHcpvItkQIPcMWQw9K6HONO/wcJ3YKRrKXDwqE38CjY00sbpsbK
ApAYrTg2uergTpc486jMeEST+0FI/dl4eKftH1Mb5Q/9RtGztqUWPrIbv7W97jTU
PXbkmvCJcXltIyh7Sw9p9rstk0JanvOf/q9RsB+JPU6K3uZLAi7dMuim8Z4WL8/
caQX7jvGfcQe9uRM0juLsWePp3YRxUCghcZlwFAHiEf6vIeJ5kh5+Og5FGXG0UY8
cpywQi/ThR2URge5ozRf59pQLJ6XP1df48CbicT2DQIDAQABoyQwIjATBgNVHSUE
DDAKBngrBgfEBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvNAQELBQAQggEBAXxs
5PlNf7Td+zZ6HuHXonbqKeCYY5HJvmPGDqkeM8J2QN+kzKtUa9XANWkeCkATED3l
xsDMUK9guK1RmvQ2gpUmZb9EsOVTME8MOBNi0GBo30qtDdCinCDhr6aXZfkI25U6
1Ttdd70IqlqxPwyfh1r9nC8kwYLT2jPZ0g0e41VQ7PRmcQDZ25hRbaBUnyQlaK0
8DNdZgWEYtMVPYB3EhlDmpVr6p/JQZPlYl7W3Jd6eOMDc9Xc1Ef7i5+6vWZDI3Ro
UCgRbHo5qVFsn0nHQWSkxkl70s40l+4ITHWc3waFgIs4DUTp8fi3Ax3VgmPmtfMDI
0Z/jxIFT0sj6GaCV8yU=
-----END CERTIFICATE-----
http-ntlm-info: to bind to 138.75.173.200:4444; - -
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 (bypass) > check
http-title: Not Found - Cannot reliably check exploitability. Is the site online and running Wo
5986/tcp open ssl http/2 syn-ack Microsoft SChannel TLS

```

Figure 12: Nmap Full scan on the known alive hosts

Based on the scan results, we only know more information about 10.0.1.11

- Ports 445,80,135, 139,443, 3389 and 5986 are open
- It resides in a domain named ArathonDomain
- Its DNS name is ARATHON-FILE.ArathonDomain.internal
- Product version is 10.0.14393 which is Windows Server 2016

3.2. Ping Sweep

I initially did a normal ping with 10.0.0.5 to see if the machine is Up. The result is that I got a ping back in response. This prompted me to launch a ping sweep using bash instead (Command: **for a in \$(seq 1 254); do (ping -c 1 10.0.0.\$a | grep "bytes from" &); done;**)

```
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 (an 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<--ck
64 bytes from 10.0.0.84: icmp_seq=1 ttl=64 time=0.311 ms<--ly. 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<--ck
64 bytes from 10.0.0.222: icmp_seq=1 ttl=64 time=0.347 ms<--ly. Is the site online and running WordPress?
```

Figure 13: Ping Sweep using Bash on 10.0.0.0/24 subnet

This time I was able to obtain 20 alive hosts, 7 more hosts than what I could obtain using Nmap. The missing ones are all the user machines detailed in the network map (10.0.0.5 – 10.0.0.11)

Did the same for the 10.0.1.0 subnet which discovered a machine with IP 10.0.1.10.

```
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
```

Did not do for the 10.0.2.0 subnet as my focus was on the 10.0.0.0 one.

4. KennyYap Client Machine (10.0.0.5)

4.1. RDP Access

In order to RDP into this machine, I did a SSH Local port forwarding to my local machine so that I could access the RDP port via my own local machine's port

4.2. Nslookup

Once I accessed the machine, I used the internal machine to do an nslookup to attempt to retrieve any domain enumeration information from the DNS server

```
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

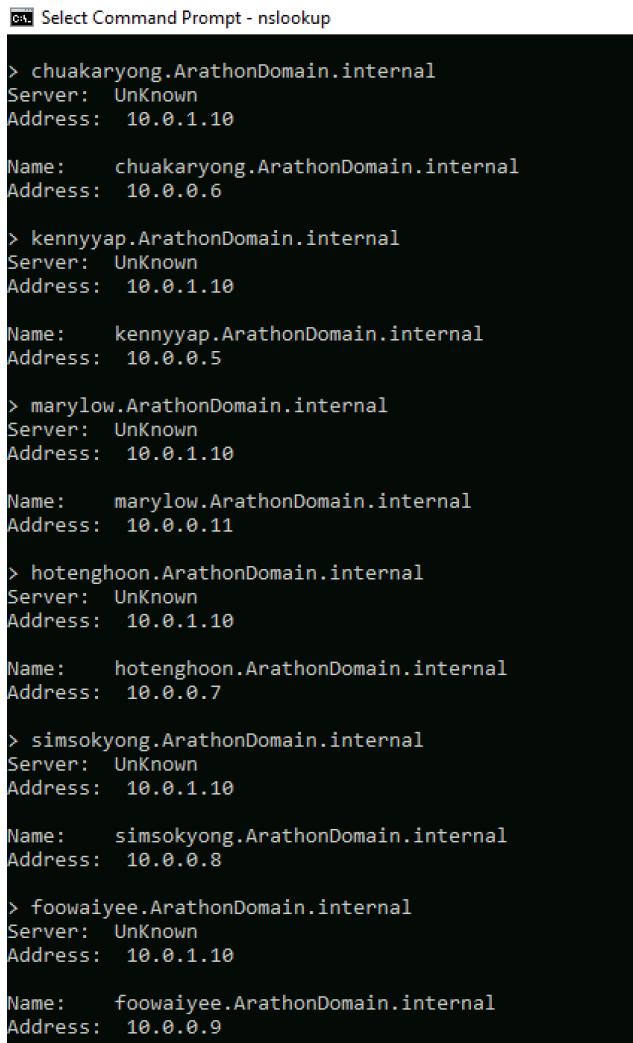
ArathonDomain.internal internet address = 10.0.1.10
ArathonDomain.internal nameserver = arathon-dc.ArathonDomain.internal
ArathonDomain.internal
    primary name server = arathon-dc.ArathonDomain.internal
    responsible mail addr = hostmaster.ArathonDomain.internal
    serial = 2682
    refresh = 900 (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
>
```

Figure 14: Nslookup information

Based on the information retrieved:

- We know that the nameserver is arathon-dc
- It has a mail server hostmaster

After knowing about the machine KennyYap, I wanted to verify that the other machines that are the names of the other users are what they are. By typing the machine names in this manner: “\$username.ArathonDomain.internal”, I was able to enumerate all the IPs of the user machines



```
ca: 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
```

Figure 15: Nslookup of User Machines

4.3. Observations

When I first entered the machine, I wanted to do some information retrieval of the user and source for any sensitive information I could find

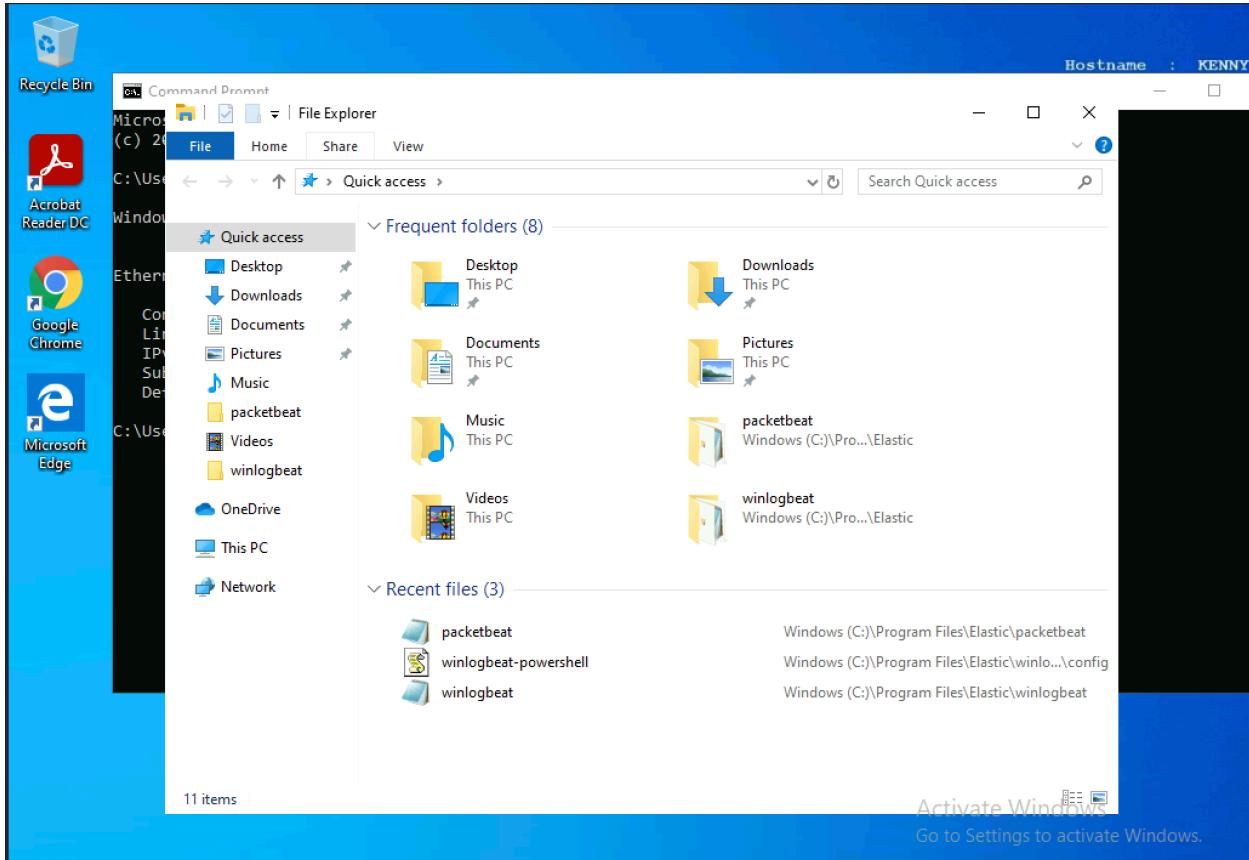


Figure 16: Windows Explorer Page

However, upon seeing the “Recent Files” of the Windows Explorer, it was very clear to me that the machine had nothing other than the WinLogBeat and PacketBeat log files within it.

Just to verify that the the PacketBeat is running, I went to check the services.

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	

Figure 17: PacketBeat Service is running

5. Domain Controller (10.0.1.10)

To enter 10.0.1.10, I did the same method of SSH Local port forwarding of the RDP port and entered it.

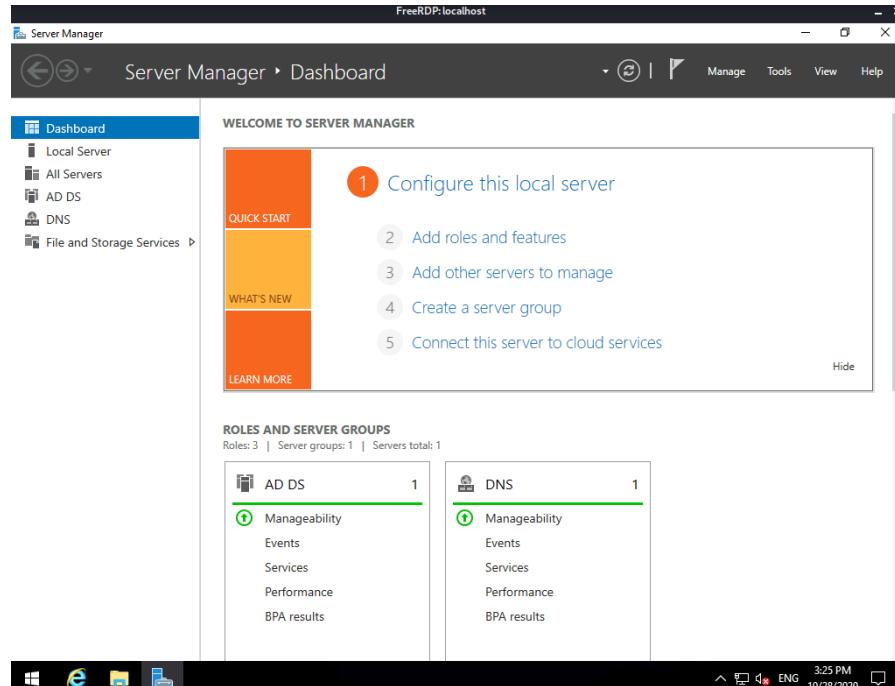


Figure 18: Windows Server Page

Opening up the Windows Server application, we can tell it is an AD and DNS server.

This Domain Controller has all the information of DNS and AD stored within the server which can be accessed via the DNS Manager and the AD Manager.

DNS Manager

File Action View Help

Forward Lookup Zones

Name Type Data Timestamp

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
dc	Host (A)	10.0.1.10	static
arathon-dc	Host (A)	10.0.1.11	10/22/2020 10:00:00 AM
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-CHNO90U	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
KennyYap	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
SPServerGE	Host (A)	10.0.1.192	10/9/2020 9:00:00 AM
SPServerJL	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

The screenshot shows the Windows Active Directory Users and Computers management console. On the left is a navigation pane with a tree view of the domain structure. The main area is a table listing computer objects, with columns for Name, Type, and Description. The table is paginated, with the current page showing entries 1 through 20 of 20 total. The entry 'CHUAKARYONG' is highlighted with a blue selection bar.

Name	Type	Description
ANGJIAYUN	Computer	
ANGZHHIN	Computer	
ARATHON-FILE	Computer	
CAROLGOH	Computer	
CHARLIECHUA	Computer	
CHOOSHUYUAN	Computer	
CHUAKARYONG	Computer	
CHUAWEEPING	Computer	
EC2AMAZ-CHNO90U	Computer	
EC2AMAZ-IBVSU50	Computer	
EC2AMAZ-JKF3VPD	Computer	
EC2AMAZ-VTV98D4	Computer	
FOOWAIYEE	Computer	
GERMAINECHOW	Computer	
HENGCHENSIANG	Computer	
HOTENGHOON	Computer	
JAMESLEE	Computer	
KENNYYAP	Computer	
LEEHIANBOON	Computer	
LEELIYI	Computer	
LIMCHENKIT	Computer	
LIMKUMKWAN	Computer	
MARYLOW	Computer	
NGYEWLING	Computer	
SEEKONGJIE	Computer	
SIMSOKYONG	Computer	
SIMWEICHYE	Computer	
SOHLIMAY	Computer	
TANKWOKLEE	Computer	
TANMAYJIA	Computer	
TANSIANGHONG	Computer	
<hr/>		
TAYBOONKHENG	Computer	
TEOHCHONGJUN	Computer	
TEOSWEEQIAN	Computer	
THOMASLEONG	Computer	
WEELINGWIN	Computer	
YEOGUANENG	Computer	

Figure 19: DNS Information

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com
 > Saved Queries
 > ArathonDomain.internal
 > Builtin
 > Computers
 > Domain Controllers
 > Employees
 > Admins
 > Staff
 > ForeignSecurityPrincipal:
 > Managed Service Account
 > Users

Name	Type	Description
Chua Kar Yong	User	
Kenny Yap	User	

Active Directory Users and Com
 > Saved Queries
 > ArathonDomain.internal
 > Builtin
 > Computers
 > Domain Controllers
 > Employees
 > Admins
 > Staff
 > ForeignSecurityPrincipal:
 > Managed Service Account
 > Users

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	

Figure 20: AD Information

If we wanted to compromise, we can dump the credentials out and use our workstation to download the files via SMB or file transfer. To make the activity less conspicuous, we could upload to the file server first and download from the file server

6. File Server (10.0.1.11)

6.1. Observations

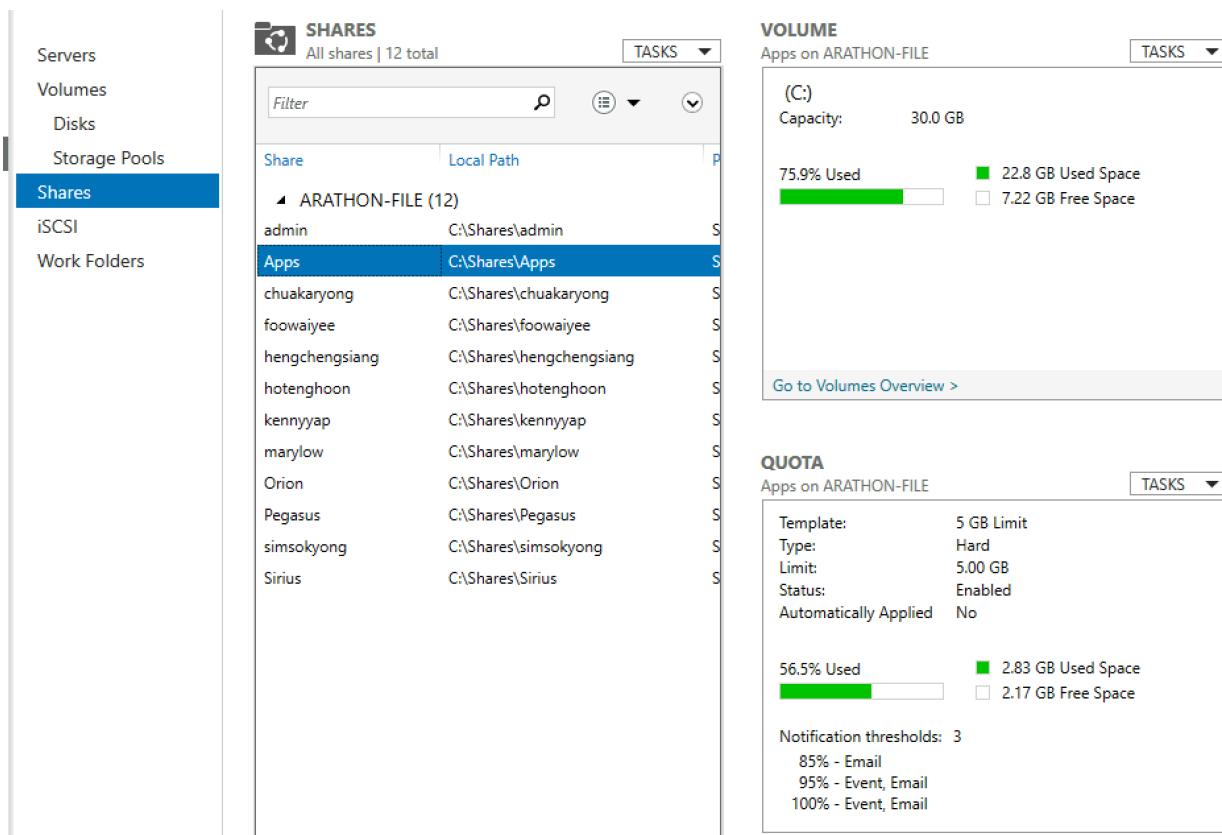


Figure 21: Shared Drive

There is a shared drive with folders made for each user done in the File Server. There is no information in all the shared folders. The only folder populated with items is the Apps folder.

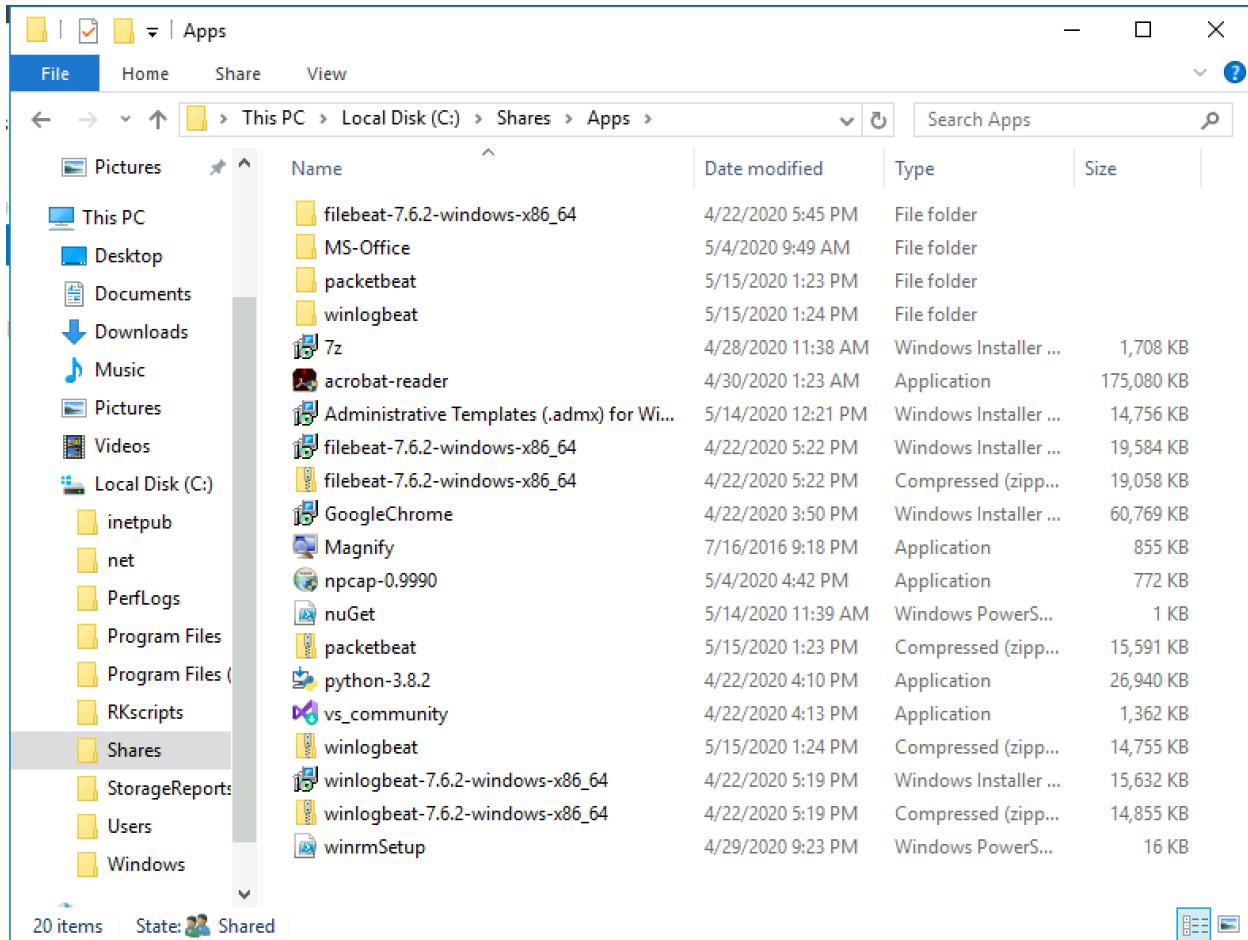


Figure 22: Apps Folder

From this folder we can identify the applications that are installed in all the Windows Clients. This does not have any sensitive information but its just a good-to-know information about the machines in the environment.

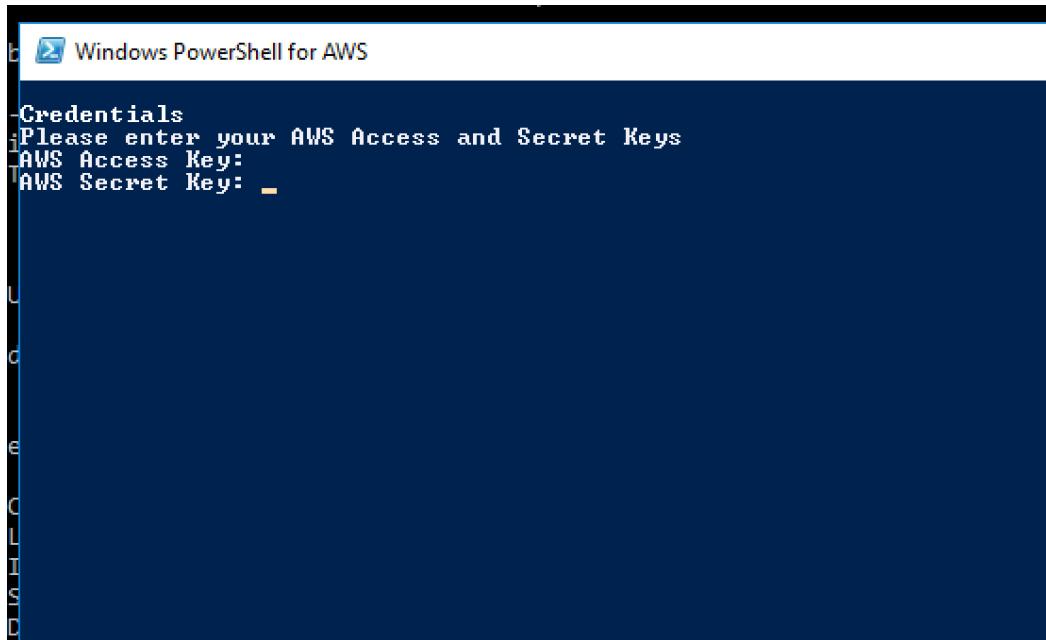


Figure 23: AWS Powershell

Another thing I felt was interesting is that there is a powershell to access the AWS console within the machine. All we would need to access the AWS control point is the Access and Secret Key.

7. Additional Observations

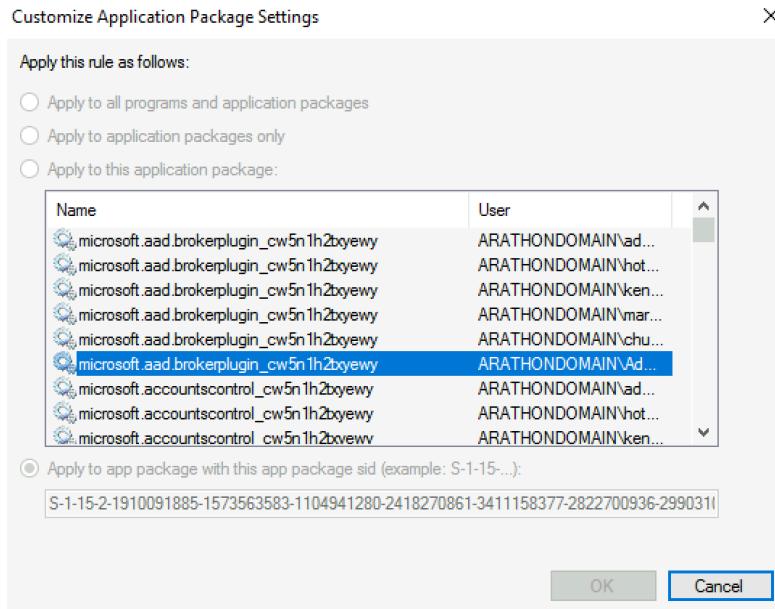
7.1. Firewall Setup

I was interested in whether there were any physical firewall nodes in the environment. A tracert from the Domain Controller to the Bastion Host showed there was only one hop made.

```
C:\Users\kennyyap>tracert 10.0.2.5  
Tracing route to 10.0.2.5 over a maximum of 30 hops  
 1  <1 ms    <1 ms    <1 ms  10.0.2.5  
Trace complete.
```

Figure 24: Tracert Result

When I took a look into the firewall configurations, I saw that the policies of inbound and outbound were not configurable. Looking into every setting, I noted that under the “Programs and Services” setting, that the applications cannot be configured as well.



This seems pretty odd for a user who has Administrator rights in the Domain but is unable to do such configurations. Thus we can infer that the configurations has to be controlled from a higher authoritative user (i.e. the AWS Manager)

8. Logs

Logs with the event and timestamps of all activities are available in the other PDF (**ArathonLogs_Lincoln.pdf**)