Arathon Technologies

Penetration Testing Report

27th October – 29th October 2020

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

Table of Contents

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 using 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: dso202O
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

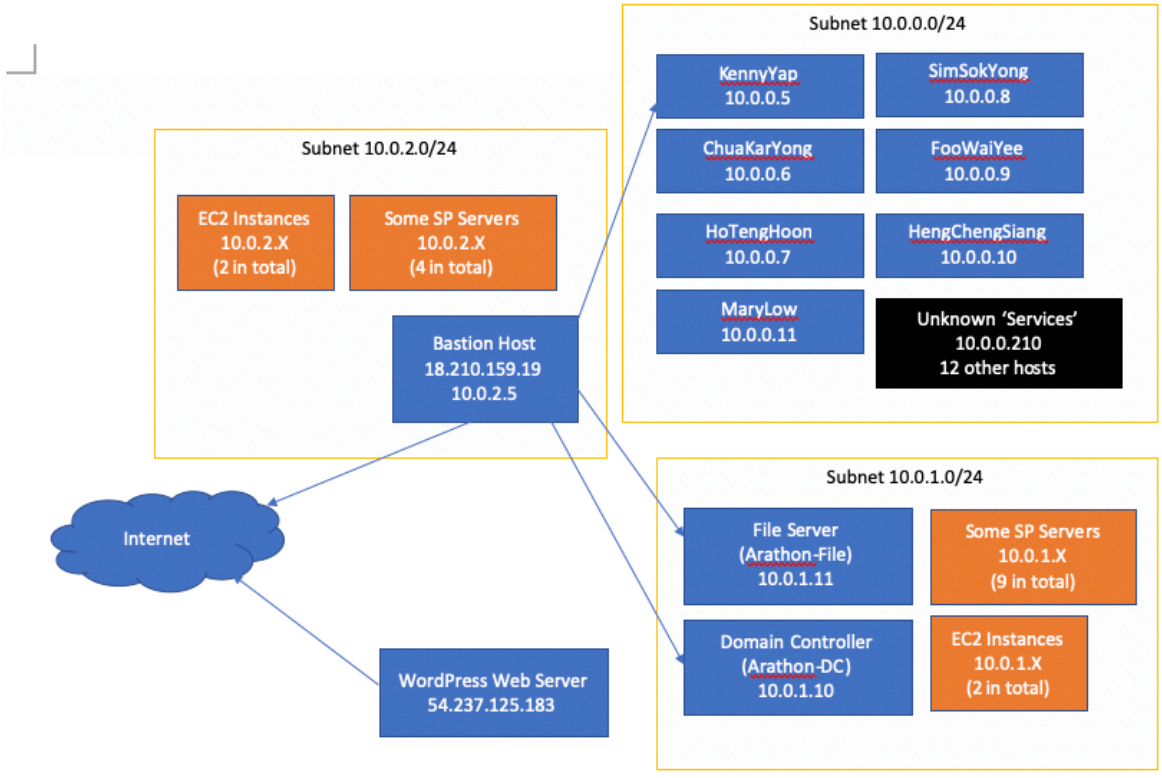


Figure 1: Network Map

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

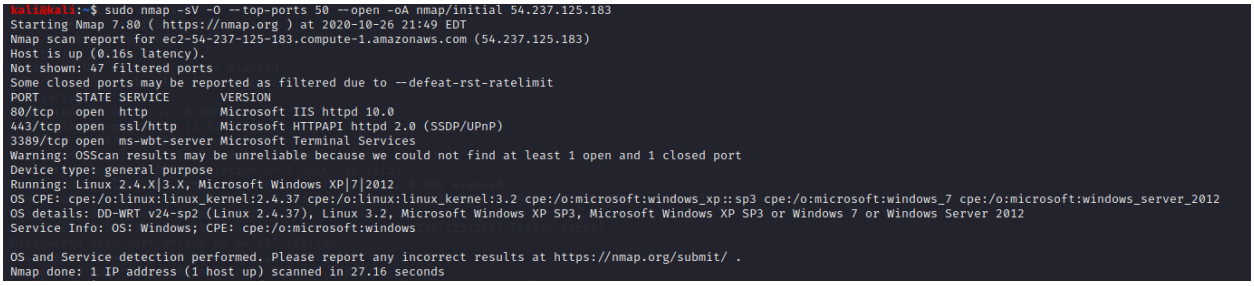
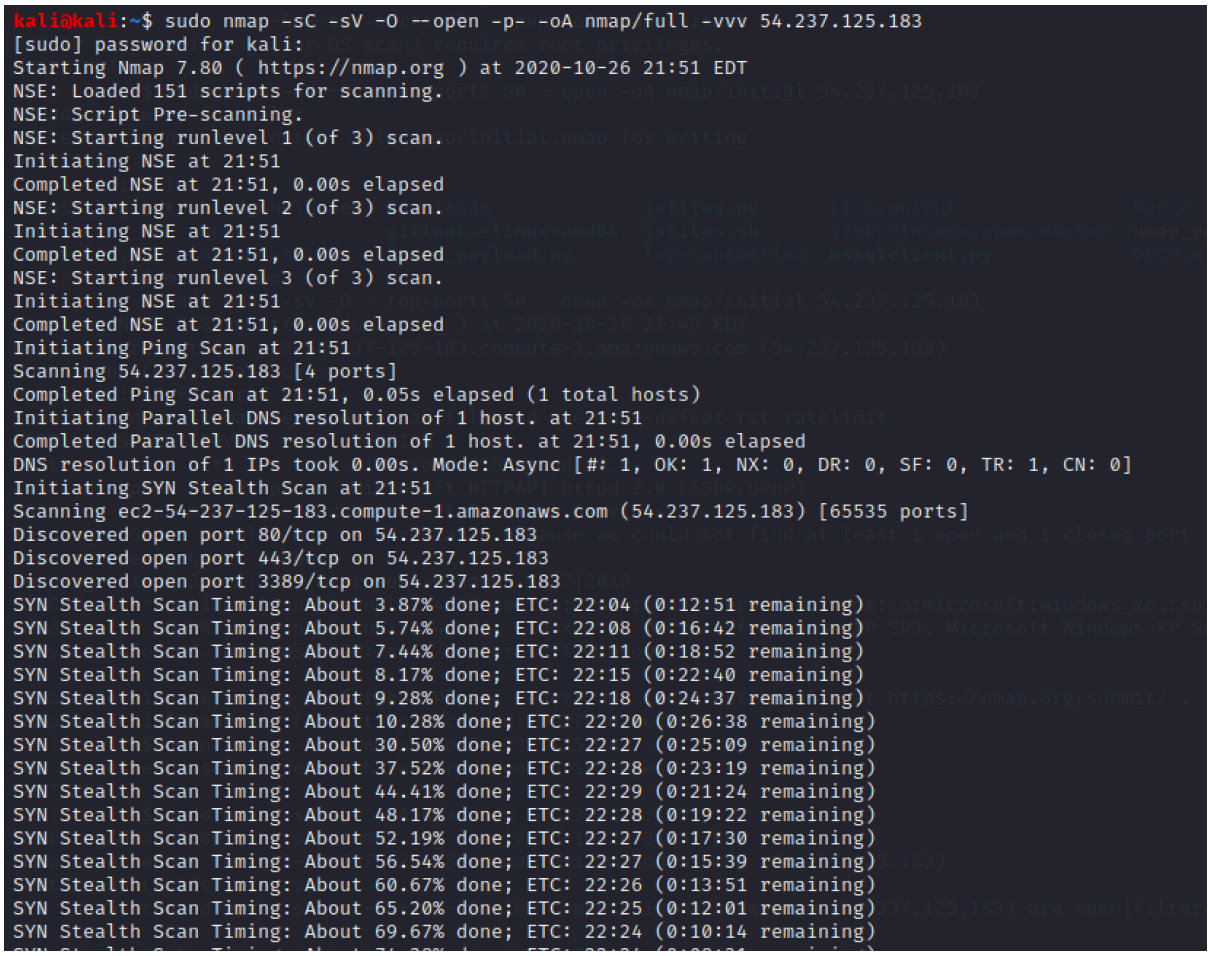
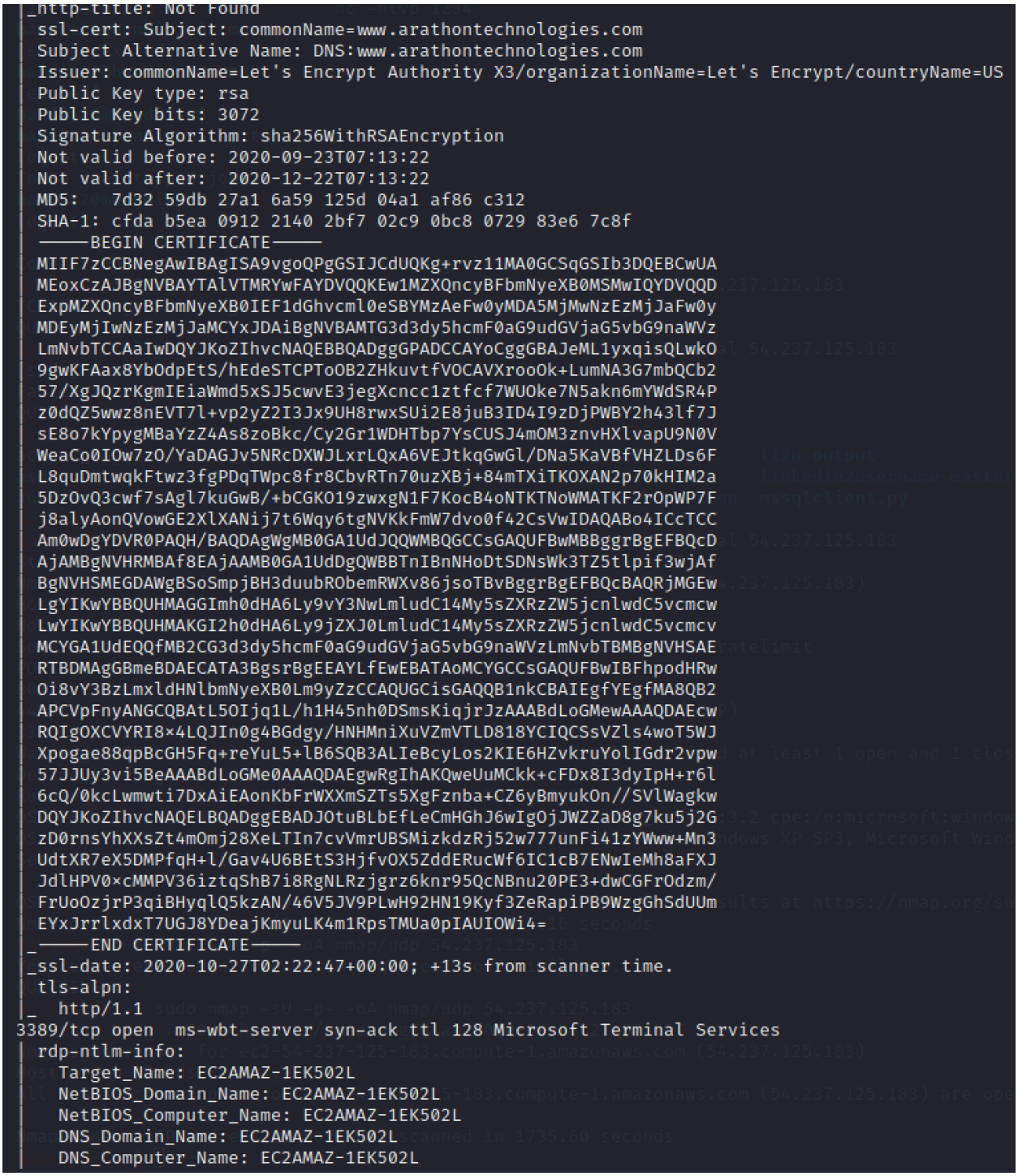


Figure 2: Initial Scan


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

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


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

```
|   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
| MRgwFgYDVQQDEw9FQzJBTUFaLTFFSzUwMkwwHhcNMjAwODI0MTI0MzA2WhcNMjEw
| MjIzMTI0MzA2WjAaMRgwFgYDVQQDEw9FQzJBTUFaLTFFSzUwMkwwggEiMA0GCSqG
| SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7ny1mAh773Wg5gPjPn9sPPd3cDyuJ5q25
| Y33sDEYF0nD/hHCJGtbYrZJk0rXUv89qBj5A8jjxh0Tt8/Yf2sQ/uQnH2TEuyBO5
| kdInsp9kPUOegwQX7OpFX9+INRH++AJcurIQZ+cb9QkXWewQtk+igABMae8NX3iH
| A+fsQbrEBveCiK1U38zVdeV8SzYpMHPaZ+nzNtEP65wSErcenDffr77l1WvP1pEM
| W/b13evT6+JEtbOOoC6HAHPIxUCsEVfsJXO+e4D4ttIfJv3nQnGywT/DCc64nlAr
| ayqLBhlepUADxInB4lw3ra926l1OZTRTzvuuCcx2A1gQHBfREbMVAgMBAAGjJDAi
| MBMGA1UdJQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIEMDANBgkqhkiG9w0BAQsF
| AAOCAQEABEKdkrn+FjytAG01D6aV3mY4QEpPNCsk2LbzzzTcaHsFA9zLW0o9PGgZ
| xwF2ixW2WSX/Drge1QPzk1Bg2W2a+pAAVGh22ujklTq832U3C7wjgut9cBRiwX6V
| d9/CYhfA42NsvdkyHyhfmaNbTz3YM6kvhVQDCFl3klnnQMfaDmwGKuppcODtPftN
| Njs0xgCxkBgcmwOKKfX/STlJBjeo2QqVUnfhhf5tdwvKrsgEh8/EJdcX5P0jKcmq
| 2O4dxBNLY/eZqAFOzQAZ/GoyqruoW5pQj9bBDOFm2nLjKIUGjVU+7GOj4OKghpcG
| PIee23sgHVQ4QicwrgVXV7tpJJMB8A==
|_-----END CERTIFICATE-----
|_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: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
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%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)

TCP Sequence Prediction: Difficulty=242 (Good luck!)
IP ID Sequence Generation: Busy server or unknown class
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

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
```

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

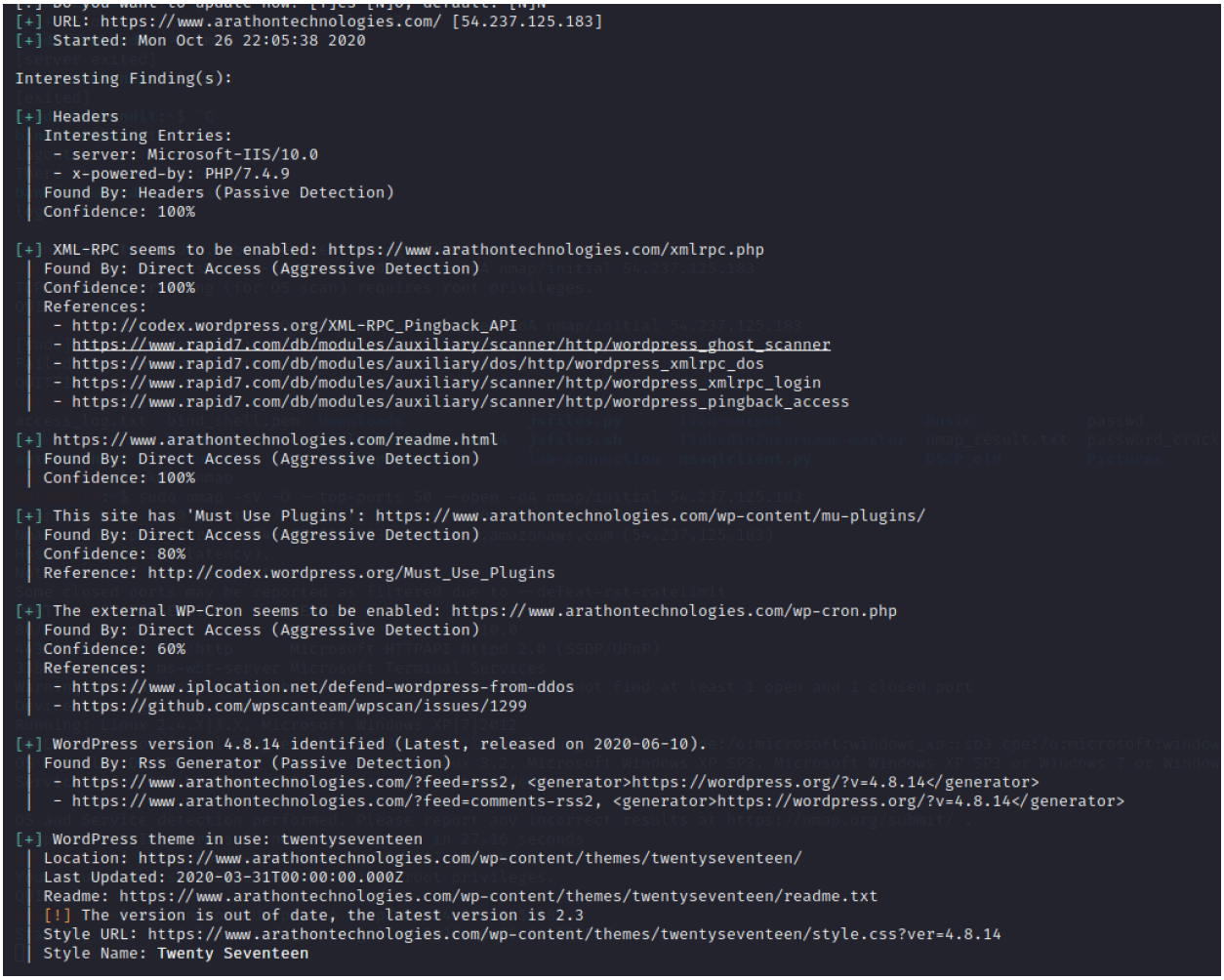


Figure 5: WPScan

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

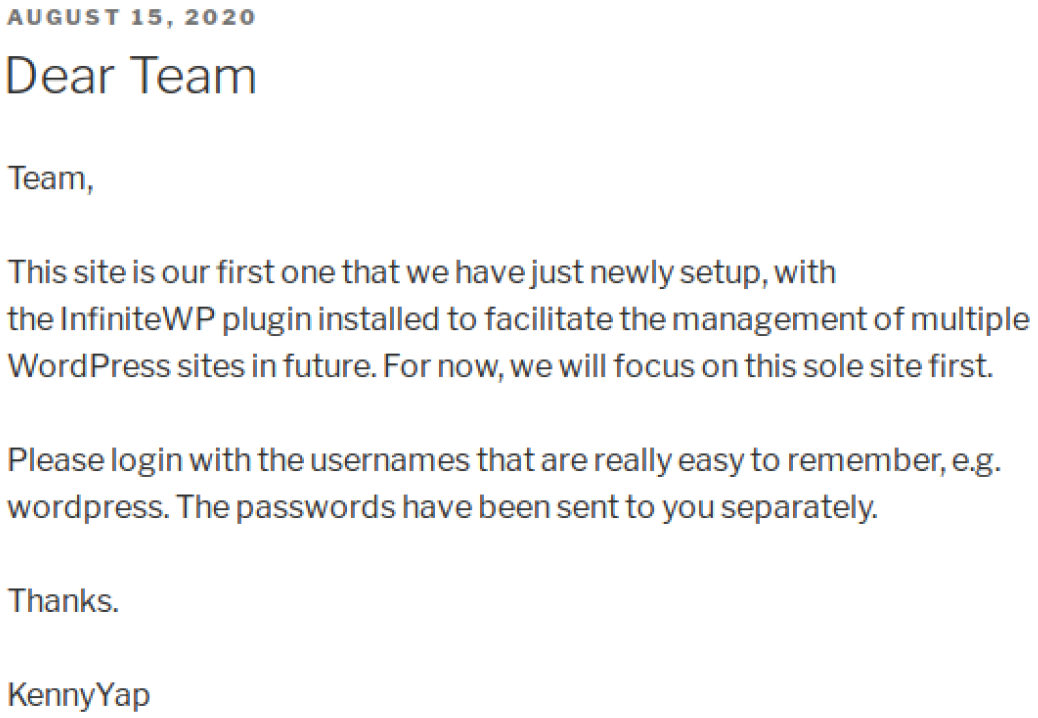
- Webpage is powered by Microsoft-IIS/10.0
- There is PHP running using version 7.4.9
- XML-RPC seems to be enabled
- WP-Cron seems to be enabled (Prevents DDoS)
- Wordpress version is 4.8.14 (latest version for 4.8 series)
- Theme is twentyseventeen (OOB version)
- No plugins are used but "Must-Use 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.

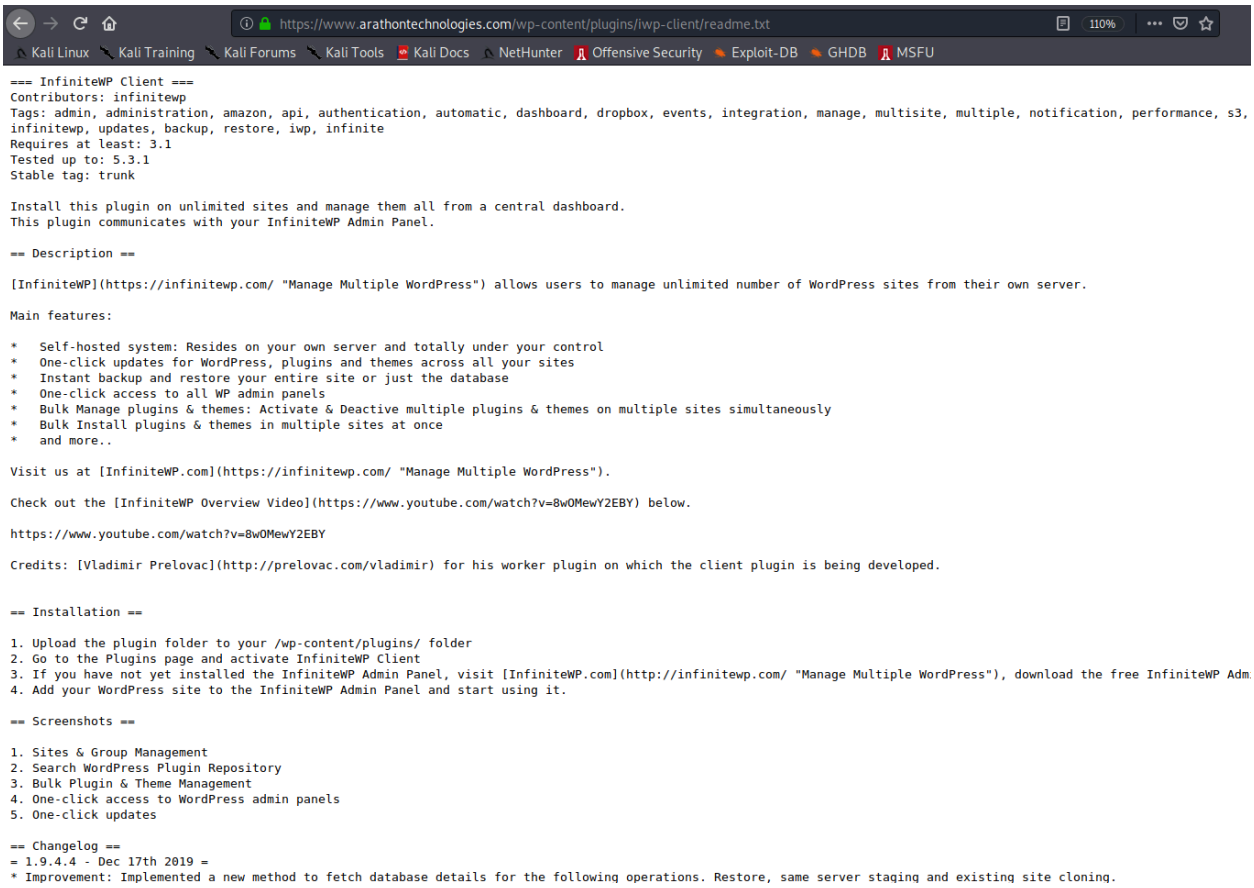


Figure 7: InfiniteWP Readme File

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=kennyyap

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.

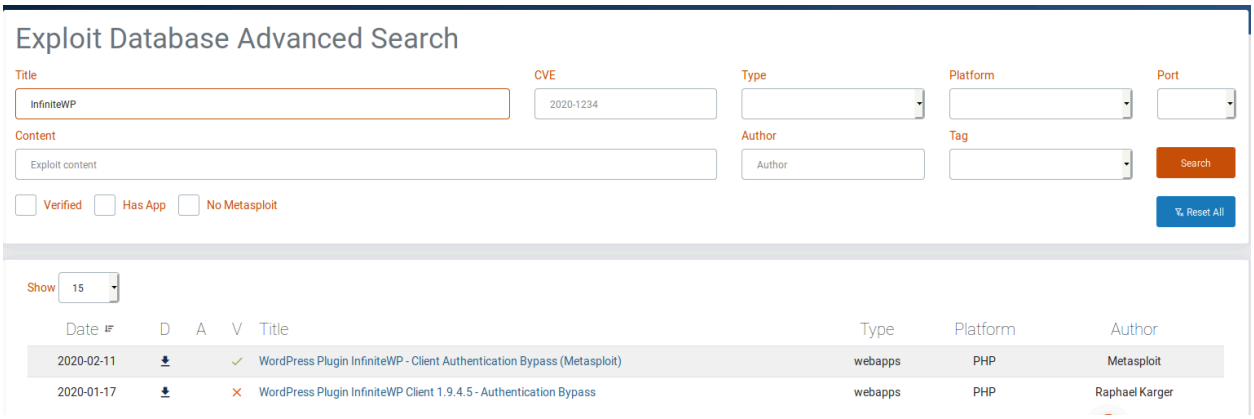


Figure 8: Exploit-DB Results on InfiniteWP

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.

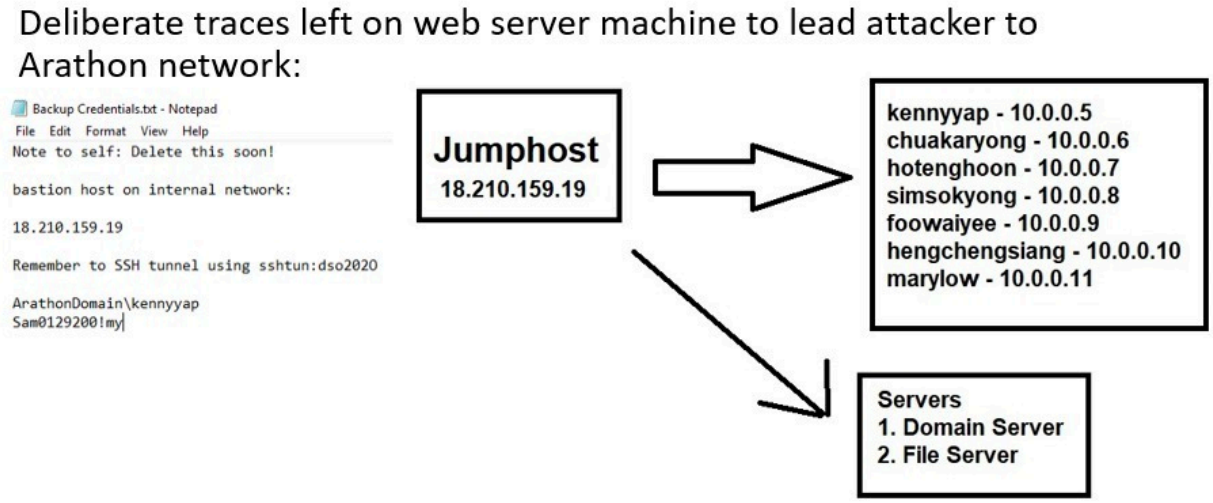


Figure 9: Credentials Given to me

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 an 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

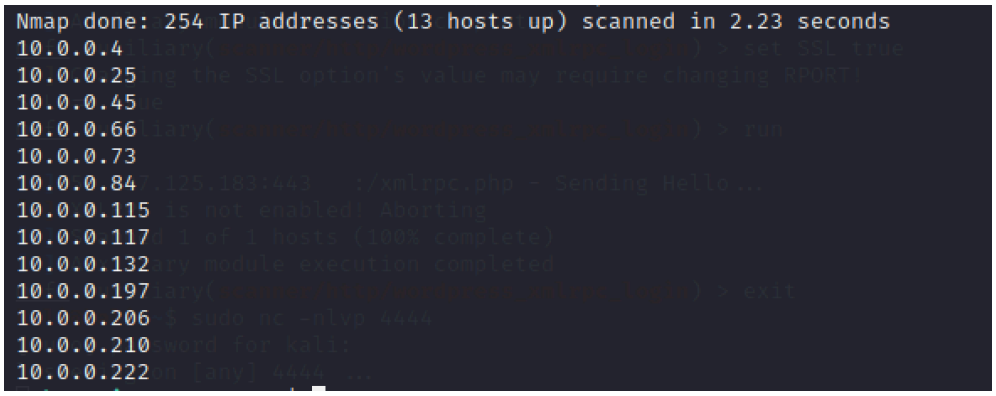


Figure 10: Nmap scan results for 10.0.0.0/24 subnet

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.

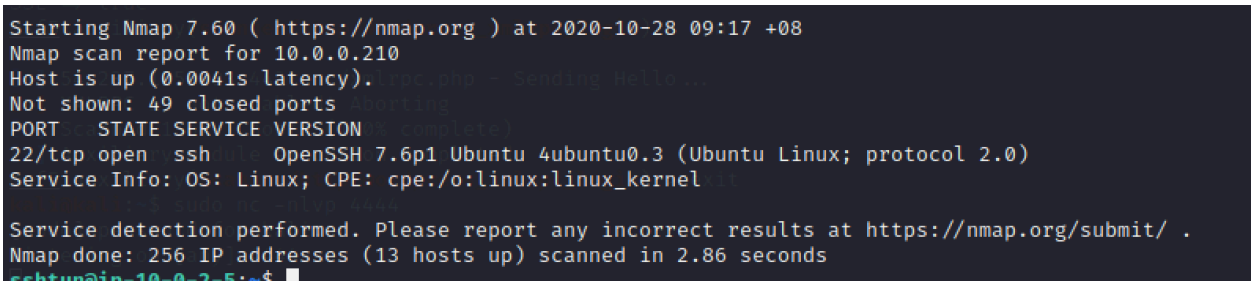
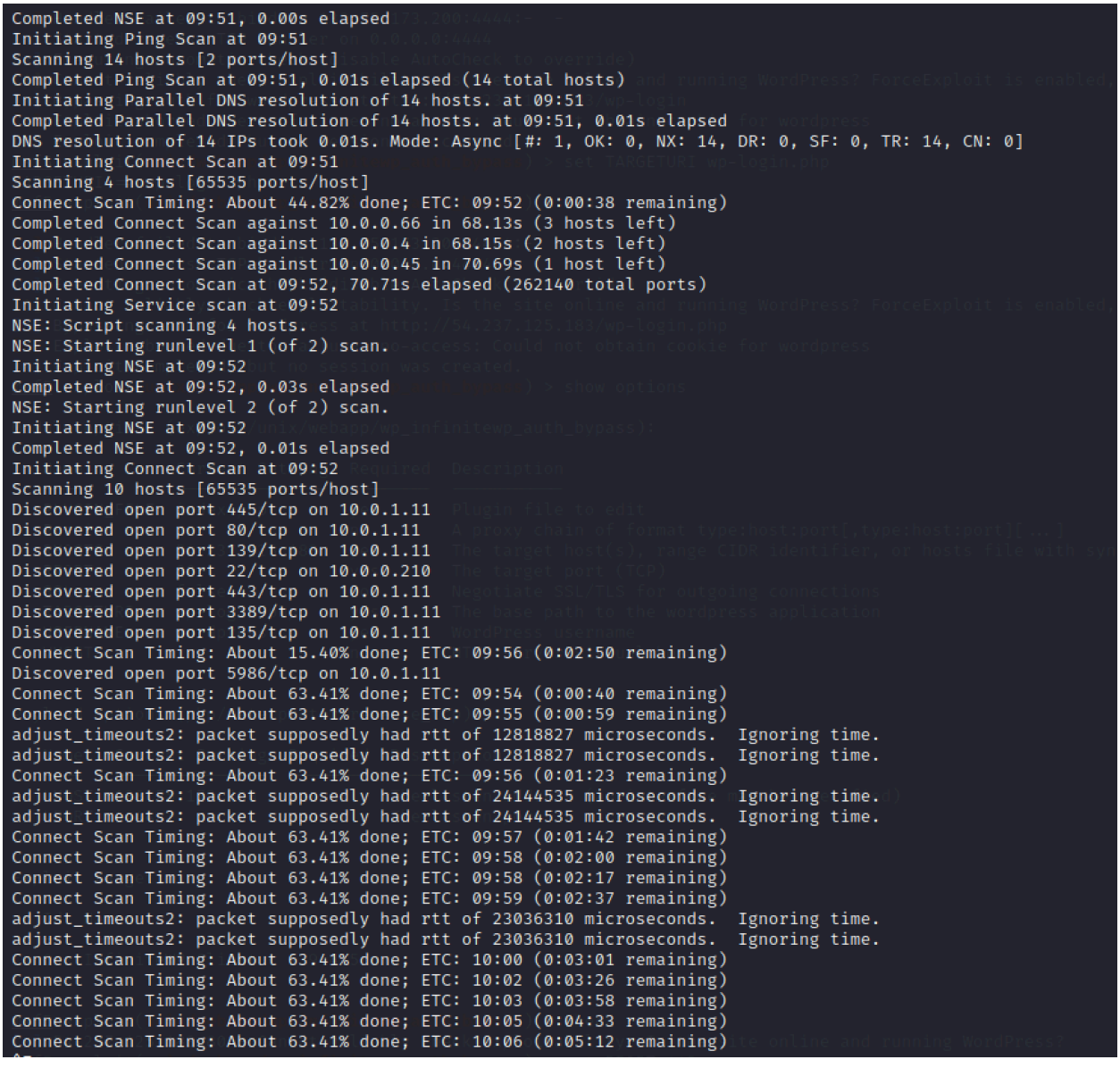


Figure 11: Initial scan on Subnet 10.0.0.0/24

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).**



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

```
Initiating Service scan at 10:21
Scanning 11 services on 10 hosts
Completed Service scan at 10:21, 53.58s elapsed (11 services on 10 hosts)
NSE: Script scanning 10 hosts.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 10:21
NSE Timing: About 99.48% done; ETC: 10:22 (0:00:00 remaining)
NSE Timing: About 99.61% done; ETC: 10:23 (0:00:00 remaining)
NSE Timing: About 99.68% done; ETC: 10:23 (0:00:00 remaining)
Completed NSE at 10:23, 90.75s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 10:23
Completed NSE at 10:23, 0.07s elapsed
Nmap scan report for 10.0.0.210
Host is up, received conn-refused (0.0041s latency).
Scanned at 2020-10-28 09:51:32 +08 for 1918s
Not shown: 65534 closed ports
Reason: 65534 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 7e:87:9b:92:2e:2d:c9:49:d3:cd:57:ac:a6:0b:7f:be (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDNKFcm13Rbe5d9rv96KZKsTNhwv/pEiISdyOed+uArVzKkyUxVZ+bIkmWZO1r3OP7Tlf/B9XUHYDiHXPucDnXVR2Witf+8w78Dp0+lLyO2QjrYVWX1t5hfRwybXsgJYMOZwb4F9GkQJNW+jI8PEgJ67hByCTs+ZrVJpKG
MsFymFgYsAYFU54jq/2i/eU2OvpDzlPfV64hrEr11dZI6oGsjz5Ot8nM5jRwkjgxtGtAiACFEZdwlpj0BRIRC8QJUzygXKiwBdMECrs9MiFdWA/fXf7Ra8htTZ52GBbv9k8RsCpdOwDih4wKWIL/yKCKuqlvZzHt9cESk+IfLsol2KUQ3
|   256 aa:69:22:08:e6:ba:7e:e2:49:eb:47:94:36:d2:68:dd (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBO4Qm4azGJBnofnXGeOyNWu1ekZyyB2dHsktyda+r5J0ZvYSWrmQJ02vsrkSjbdRRgTeNDyY/umDSXzbXK9NGwc=
|   256 d5:20:cd:1e:5c:97:40:87:f1:ee:dd:b3:42:c0:ee:10 (EdDSA)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ3vIloU6wvCN84IcITzPumkyasf2Tfv01LX4AcA+bbq
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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

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

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

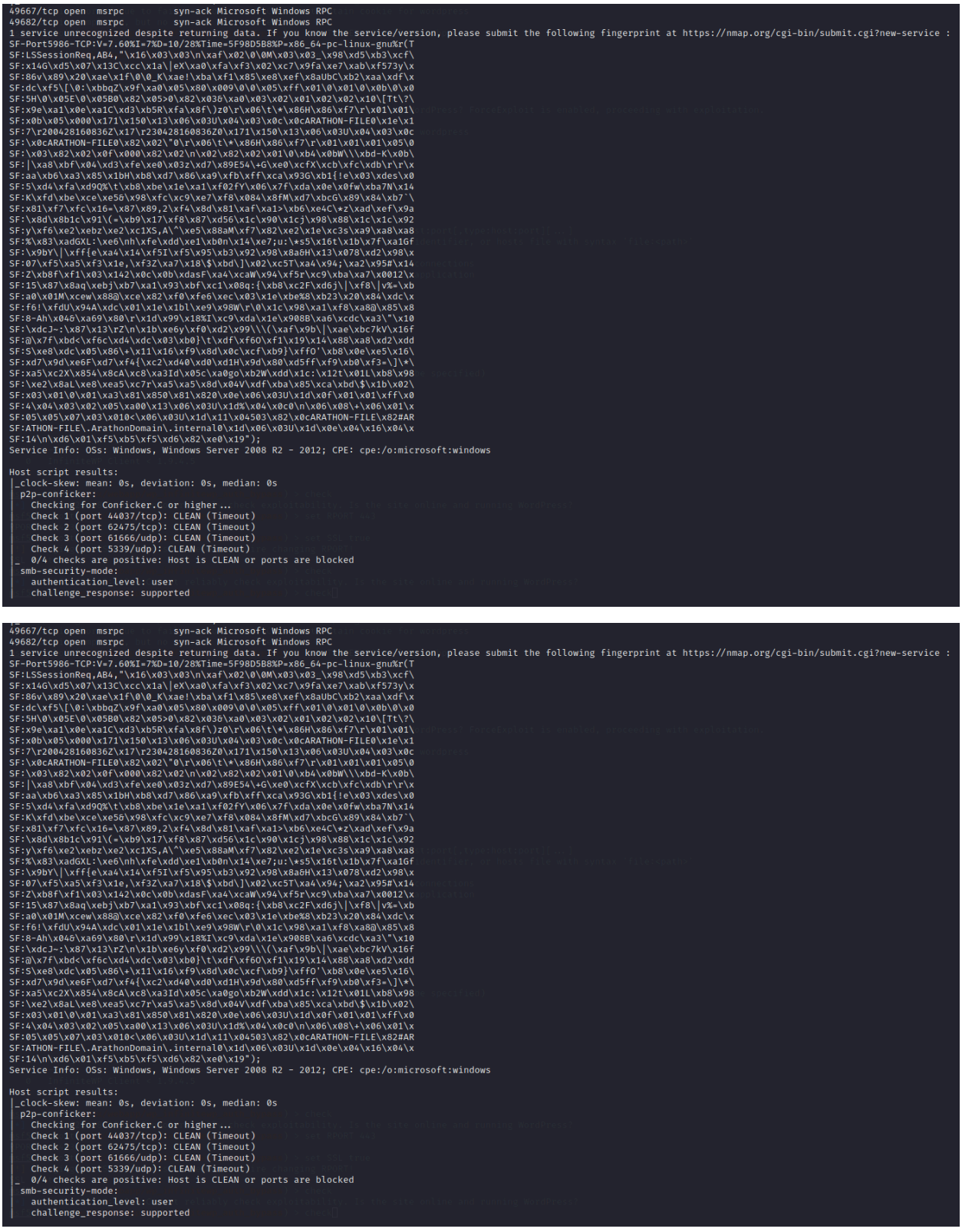


Figure 12: Nmap Full scan on the known alive hosts

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;**)

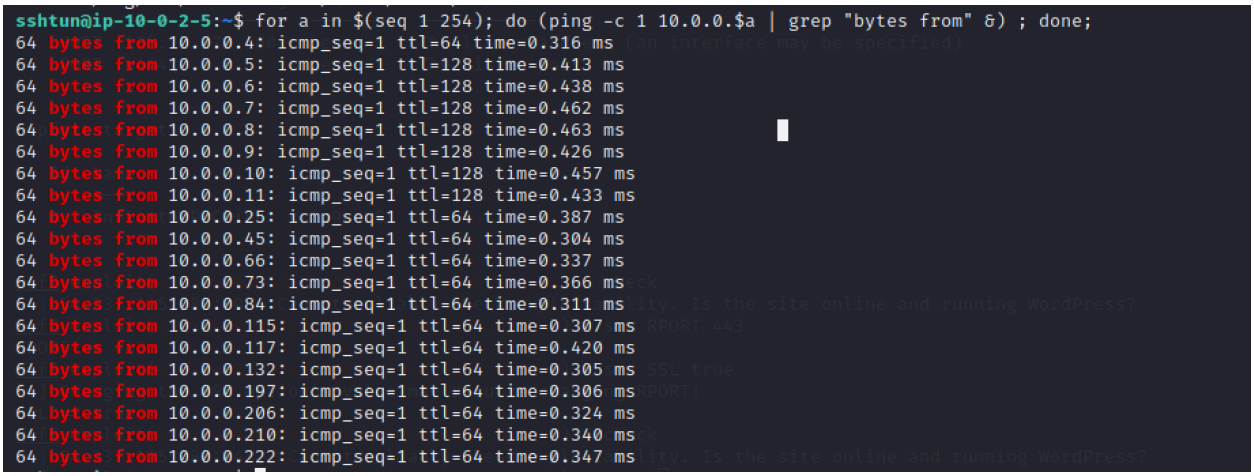
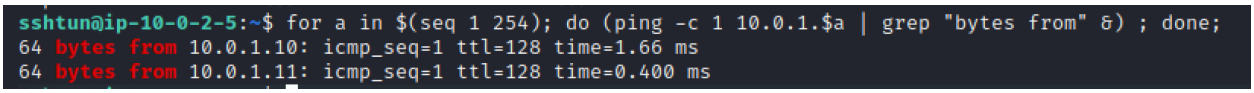


Figure 13: Ping Sweep using Bash on 10.0.0.0/24 subnet

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.



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

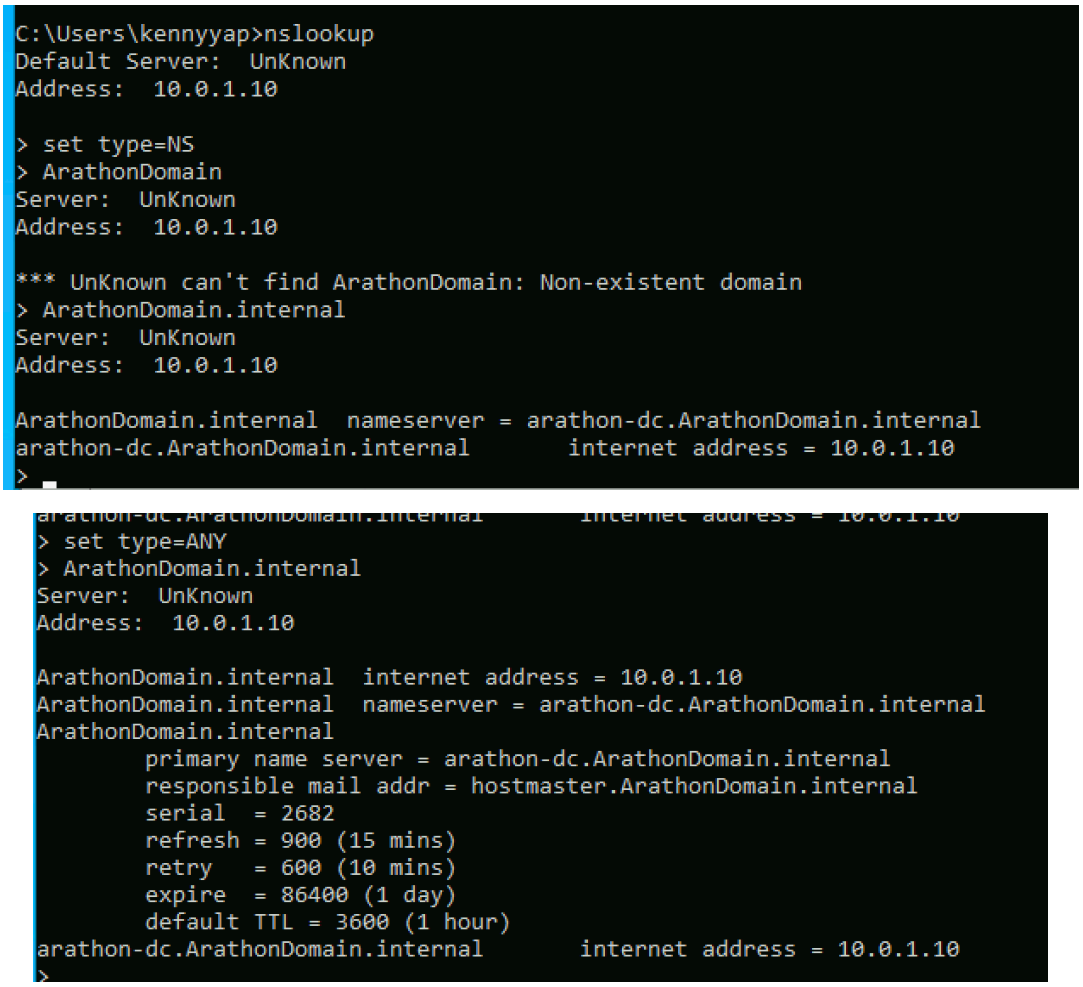


Figure 14: Nslookup information

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

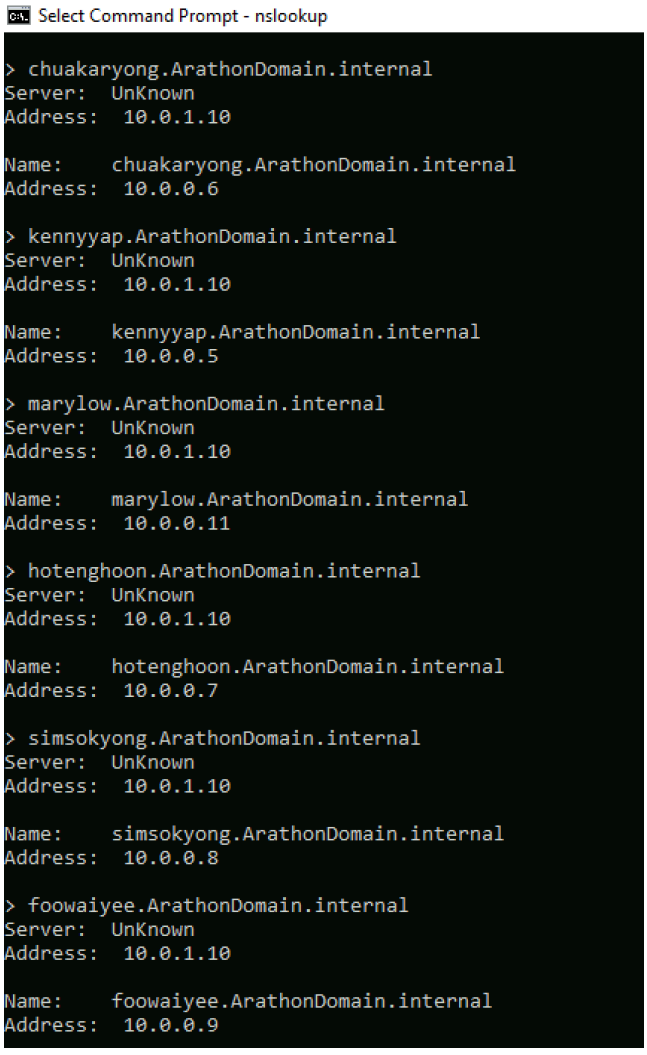


Figure 15: Nslookup of User Machines

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

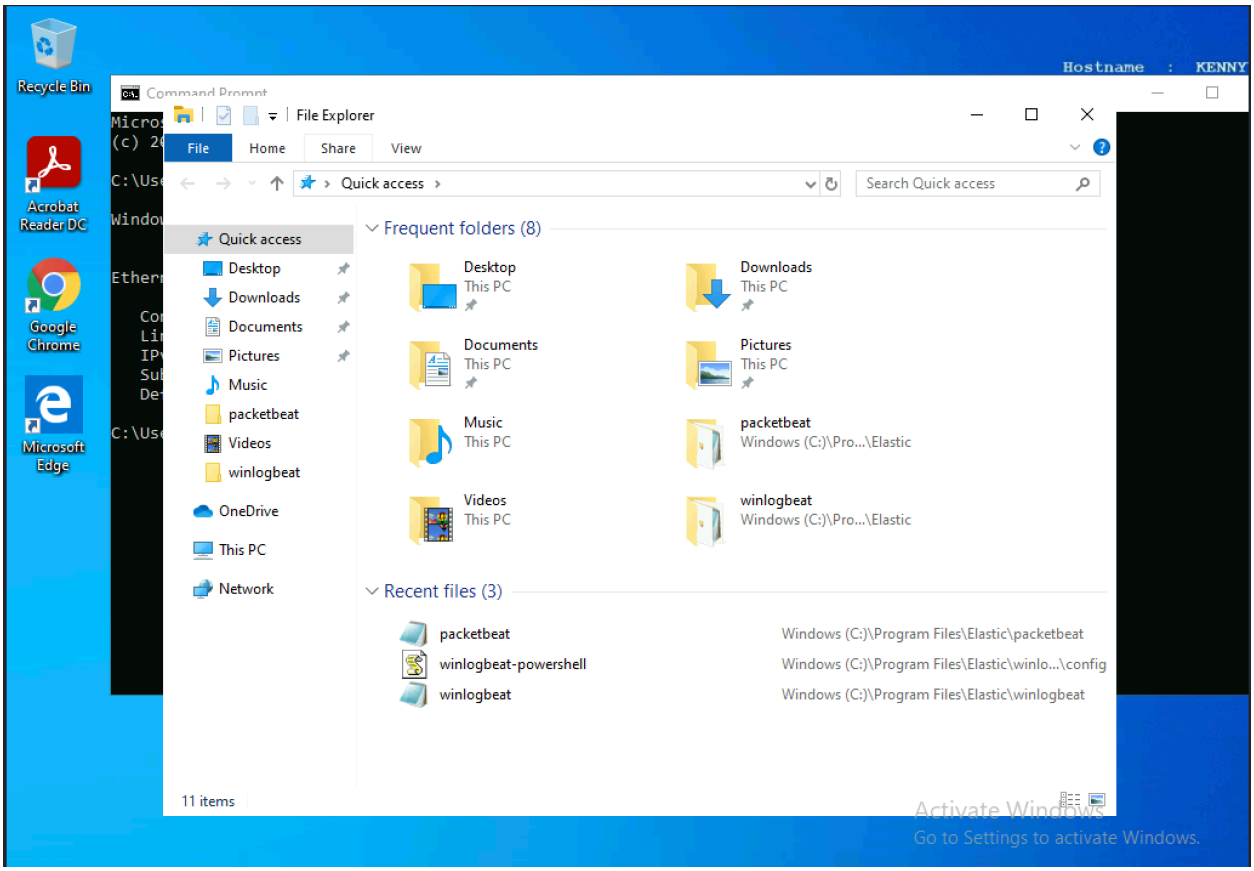


Figure 16: Windows Explorer Page

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.

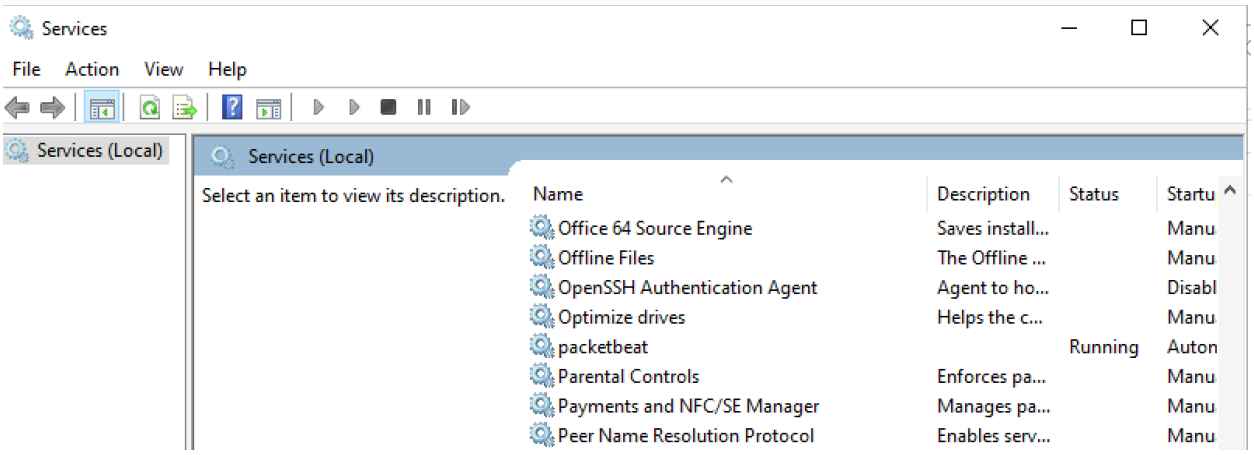


Figure 17: PacketBeat Service is running

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.

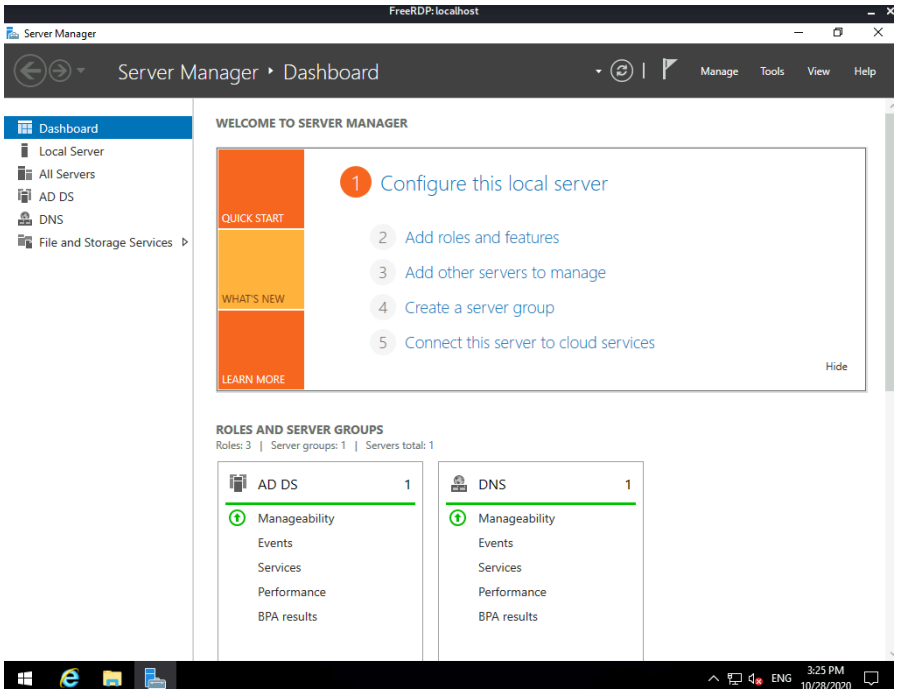
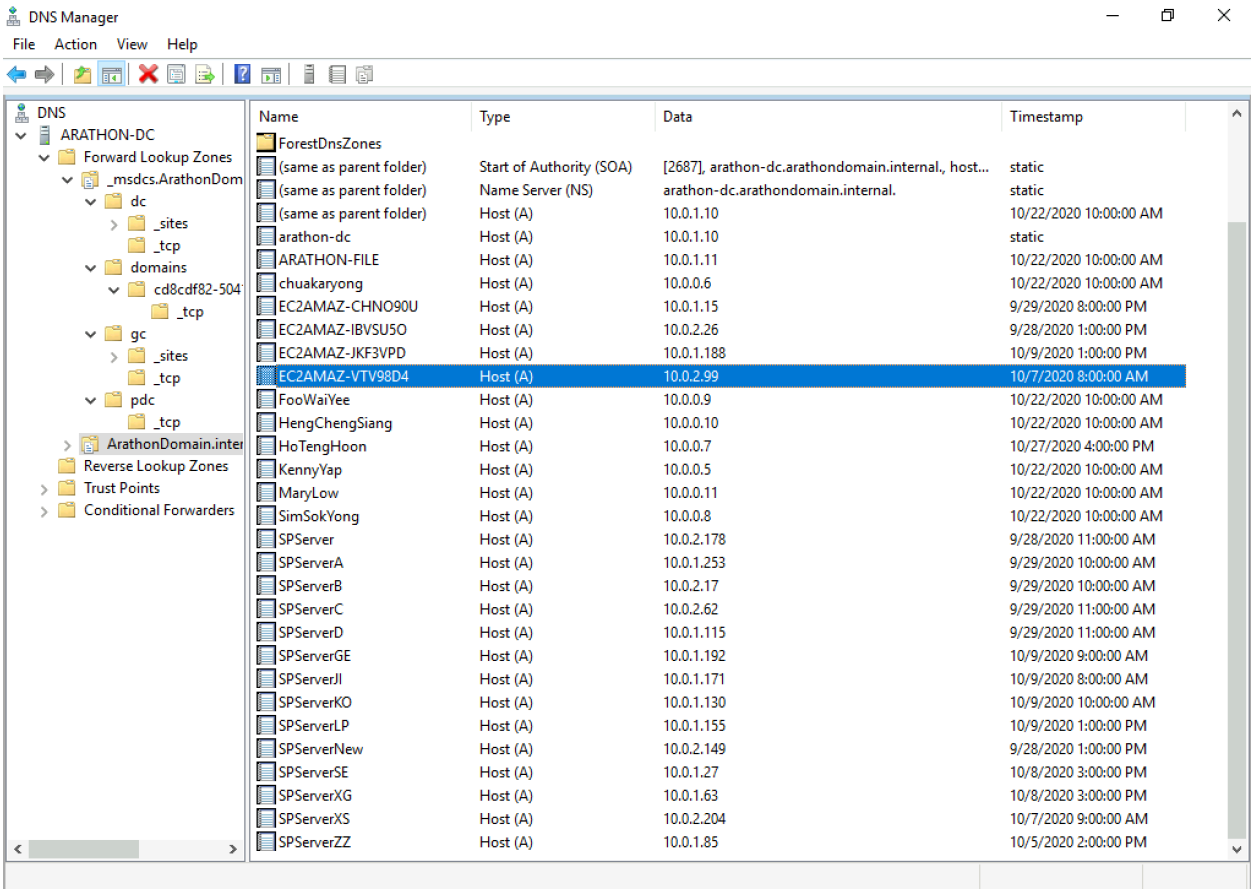


Figure 18: Windows Server Page

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
DNS
ARATHON-DC
Forward Lookup Zones
_msdcs.ArathonDom
dc
_sites
_tcp
domains
cd8cdf82-504
_tcp
gc
_sites
_tcp
pdc
_tcp
ArathonDomain.inter
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name Type Data Timestamp
ForestDnsZones
(same as parent folder) 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-CHNO90U Host (A) 10.0.1.15 9/29/2020 8:00:00 PM
EC2AMAZ-IBVSU5O 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
SPServerJI 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

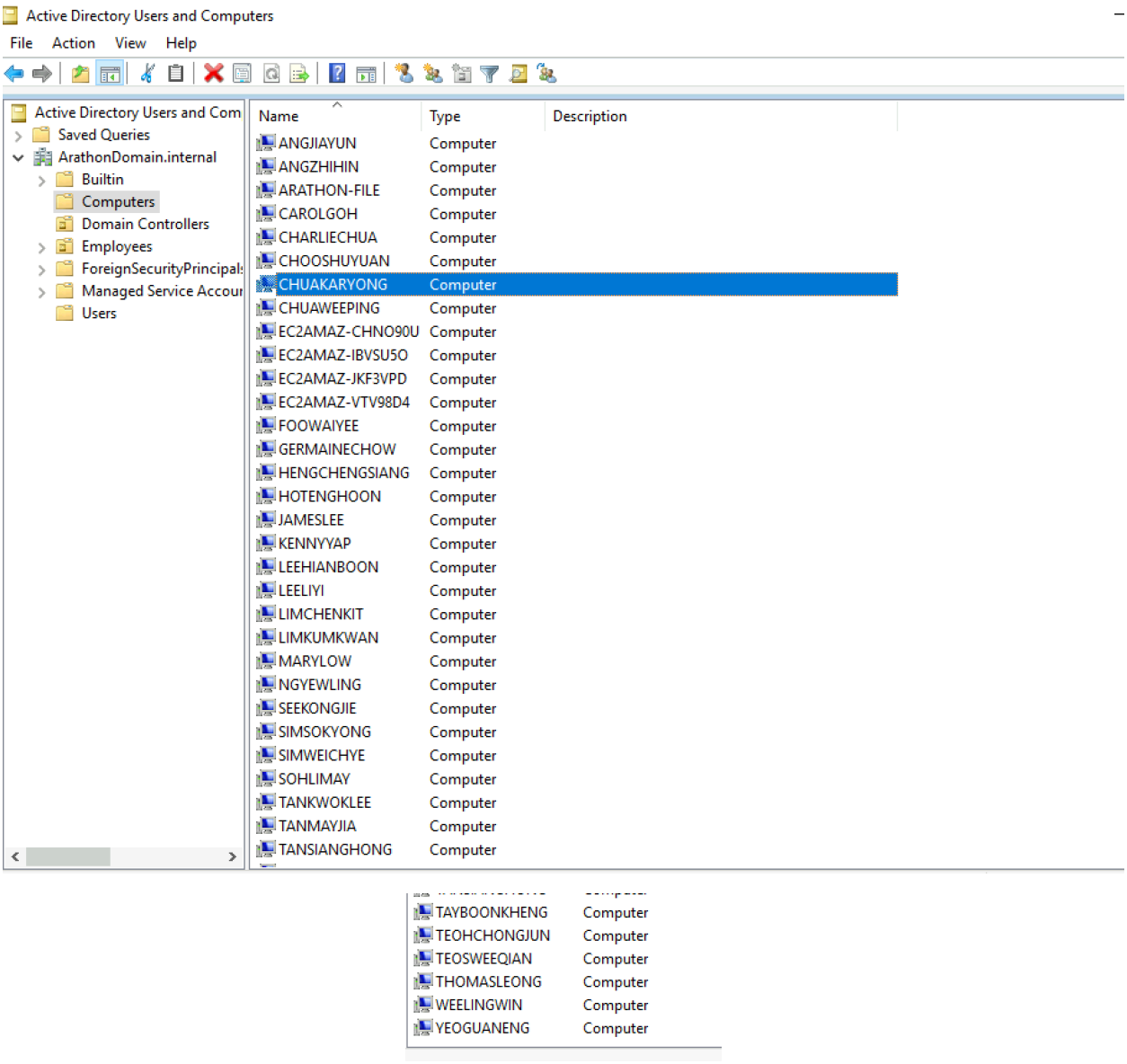


Figure 19: DNS Information

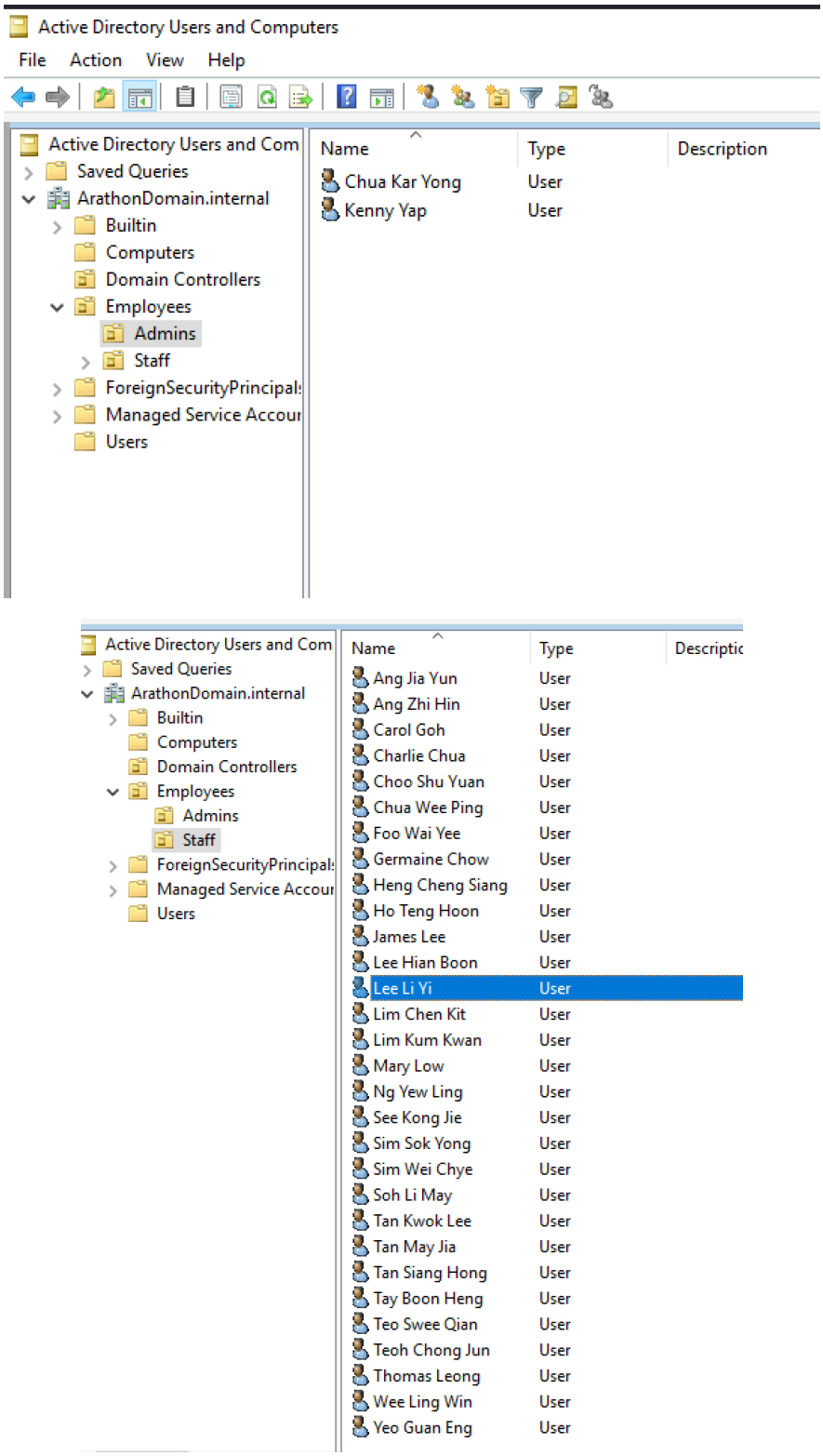


Figure 20: AD Information

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

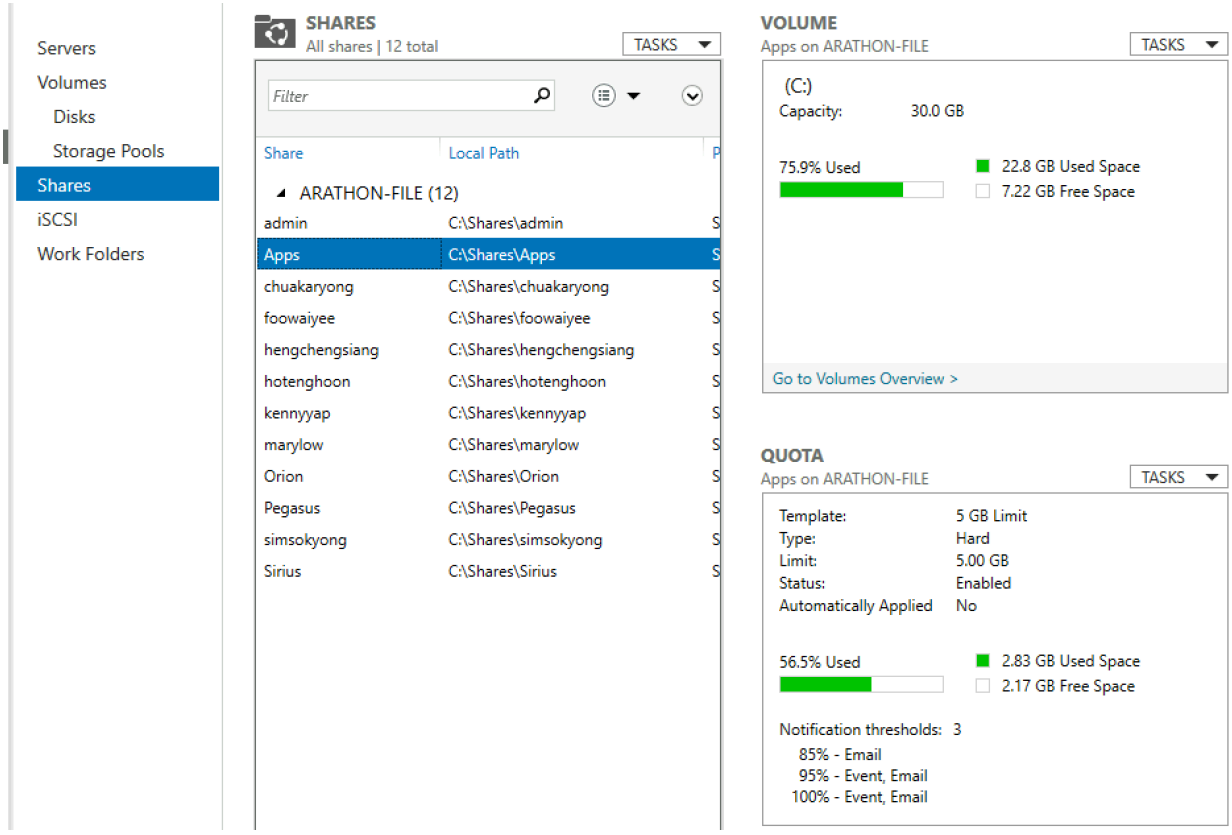


Figure 21: Shared Drive

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.

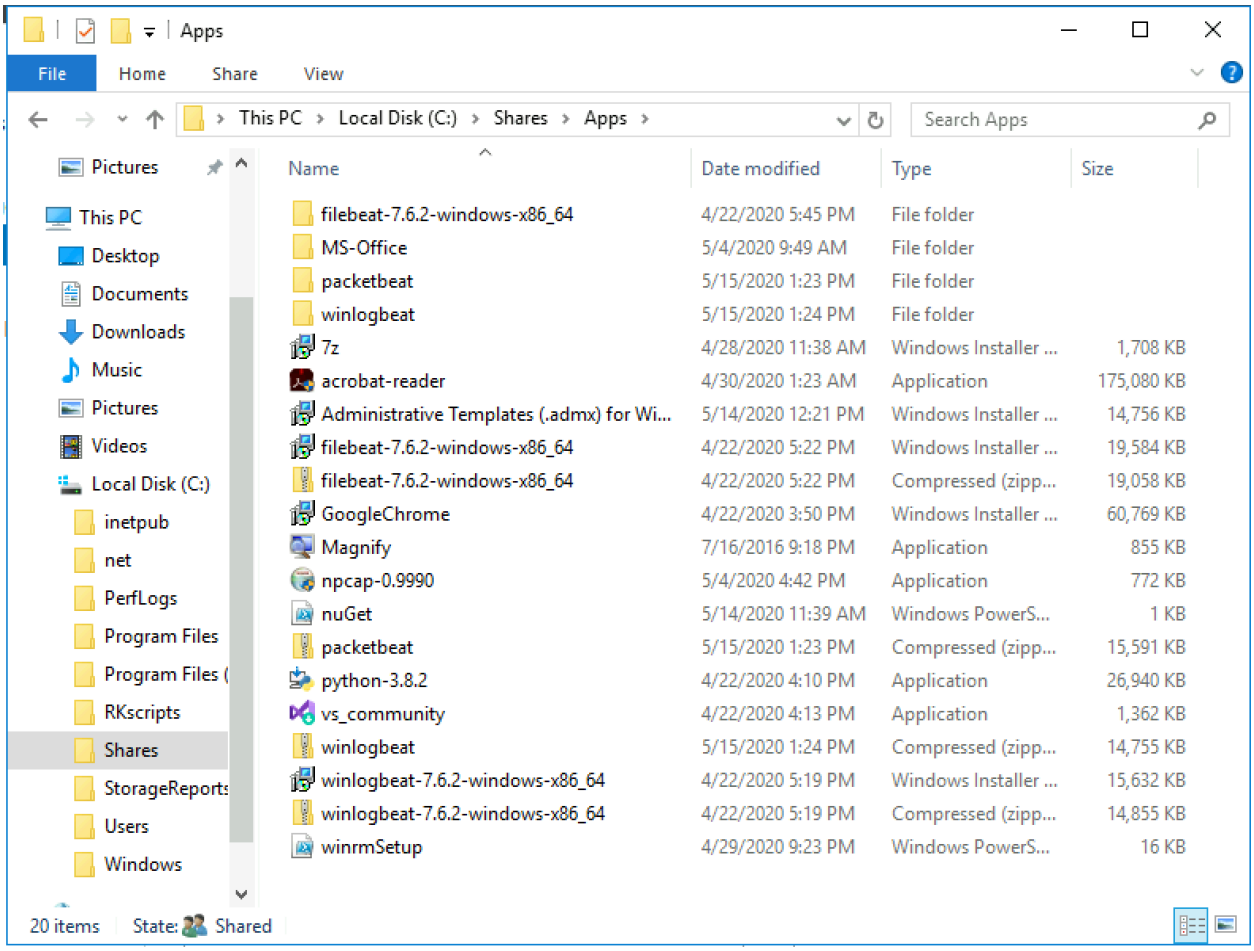


Figure 22: Apps Folder

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.

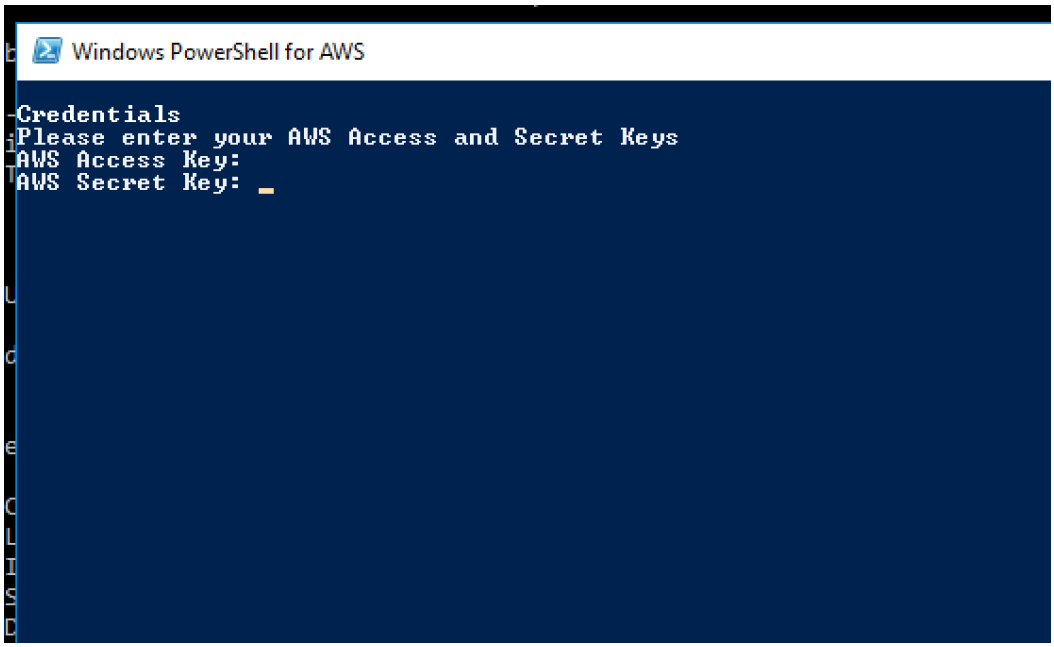


Figure 23: AWS Powershell

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

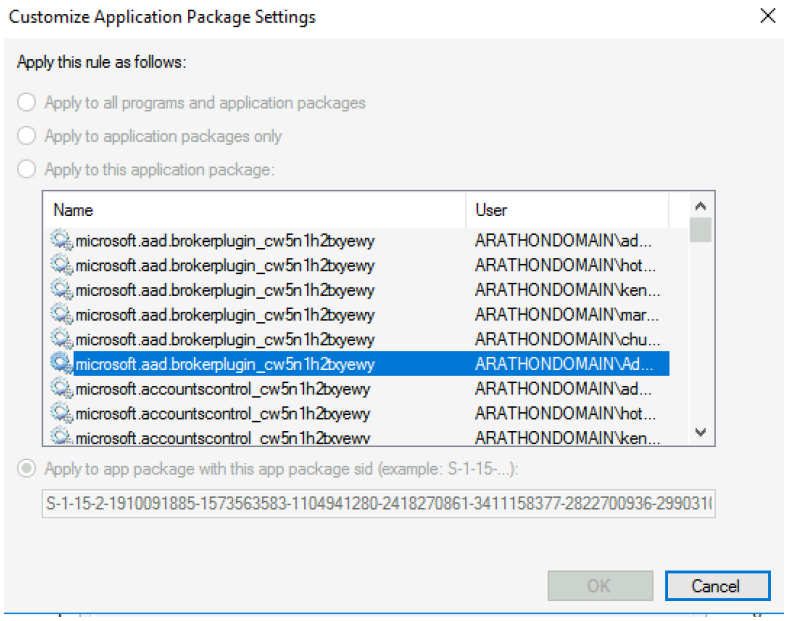
7.1. Firewall Setup

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**)