Post Exploitation – Discovering Network Information In Windows

pentestlab.blog/category/post-exploitation/page/9

December 17, 2012

In network infrastructure penetration tests if we manage to exploit one system then it is easy to obtain information for the network that this system is part of.This information is important because in almost every network penetration test the ultimate goal is to become domain administrator and in order to achieve that it is necessary to know the appropriate commands that will help us to gather information about the network that we are already inside.In this article we will see how we can gather information about windows networks that we are conducting the penetration test from the system that we have already exploited.

Lets say that we have exploited a windows system and we want to know more about the network that this system belongs to.The first and most common command is of course the **ipconfig /all** which it will display to us all the information about the network adapters of the host and the Windows IP configuration as the picture below is showing:

```
C:\WINDOWS\system32>ipconfig /all
ipconfig /all

Windows IP Configuration

        Host Name . . . . . . . . . . . . : MAROON
        Primary Dns Suffix  . . . . . . . : london.training.nta-monitor.com
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : london.training.nta-monitor.com
                                            localdomain
                                            training.nta-monitor.com
                                            nta-monitor.com

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : localdomain
        Description . . . . . . . . . . . : VMware Accelerated AMD PCNet Adapter #2
        Physical Address. . . . . . . . . : 00-50-56-BB-00-87
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 172.16.212.128
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.212.2
        DHCP Server . . . . . . . . . . . : 172.16.212.254
        DNS Servers . . . . . . . . . . . : 172.16.212.2
        Primary WINS Server . . . . . . . : 172.16.212.2
        Lease Obtained. . . . . . . . . . : Tuesday, December 11, 2012 12:41:58 AM
        Lease Expires . . . . . . . . . . : Tuesday, December 11, 2012 1:11:58 AM
```

ipconfig /all

Another command is the **ipconfig /displaydns** which it will display the contents of local DNS cache.

```
C:\WINDOWS\system32>ipconfig /displaydns
ipconfig /displaydns

Windows IP Configuration

        1.0.0.127.in-addr.arpa
        ----------------------------------------
        Record Name . . . . . : 1.0.0.127.in-addr.arpa.
        Record Type . . . . . : 12
        Time To Live  . . . . : 598076
        Data Length . . . . . : 4
        Section . . . . . . . : Answer
        PTR Record  . . . . . : localhost


        _ldap._tcp.dc._msdcs.london.training.nta-monitor.com
        ----------------------------------------
        No records of type SRV


        _ldap._tcp.1d41f2e6-232b-45d0-be89-681bb6bf2405.domains._msdcs.london.training.nta-
monitor.com
        ----------------------------------------
        No records of type SRV


        localhost
        ----------------------------------------
        Record Name . . . . . : localhost
        Record Type . . . . . : 1
        Time To Live  . . . . : 598076
        Data Length . . . . . : 4
        Section . . . . . . . : Answer
        A (Host) Record . . . : 127.0.0.1
```

Display Local DNS Cache

Systems in internal networks most of the times contain shared folders which can be listed with the command **net share**.

```
C:\WINDOWS\system32>net share
net share

Share name   Resource                        Remark

-------------------------------------------------------------------------------
ADMIN$       C:\WINDOWS                      Remote Admin
C$           C:\                             Default share
IPC$                                         Remote IPC
The command completed successfully.
```

System Shares

We might also want to discover other internal networks that exist by examining the machine routing table with the command **route print**.

```
C:\WINDOWS\system32>route print
route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 56 bb 00 87 ...... VMware Accelerated AMD PCNet Adapter #2 - Packet Scheduler M
iniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.212.2  172.16.212.128      10
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
     172.16.212.0    255.255.255.0   172.16.212.128  172.16.212.128      10
   172.16.212.128  255.255.255.255        127.0.0.1       127.0.0.1      10
   172.16.255.255  255.255.255.255   172.16.212.128  172.16.212.128      10
        224.0.0.0        240.0.0.0   172.16.212.128  172.16.212.128      10
  255.255.255.255  255.255.255.255   172.16.212.128  172.16.212.128       1
Default Gateway:      172.16.212.2
===========================================================================
Persistent Routes:
  None
```

Routing Table

The **ARP -A** command will list all the systems that are currently in the machine's ARP table helping us to discover other valid hosts.

```
C:\WINDOWS\system32>ARP -A
ARP -A

Interface: 172.16.212.128 --- 0x2
  Internet Address      Physical Address      Type
  172.16.212.1          00-50-56-c0-00-08     dynamic
  172.16.212.2          00-50-56-f8-4f-84     dynamic

C:\WINDOWS\system32>
```

ARP Table

We can also use the network diagnostic command of the system to obtain information about operating system,network adapters,network clients and other network configuration with the command **netsh diag show all**.

```
C:\WINDOWS\system32>netsh diag show all
netsh diag show all

Default Outlook Express Mail (Not Configured)

Default Outlook Express News (Not Configured)

Internet Explorer Web Proxy (Not Configured)

Loopback (127.0.0.1)

Computer System (MAROON)

Operating System (Microsoft Windows XP Professional)

Version (5.1.2600)

Modems

Network Adapters
     1. [00000001] VMware Accelerated AMD PCNet Adapter
     2. [00000010] VMware Accelerated AMD PCNet Adapter

Network Clients
     1. VMware Shared Folders
     2. Microsoft Terminal Services
     3. Microsoft Windows Network
     4. Web Client Network
```

network diagnostic

Another information that is important to learn about the host that we have exploited is to see which other hosts are on the same workgroup.The command that we will need to type is the **net view**.

```
C:\WINDOWS\system32>net view
net view
Server Name            Remark

-------------------------------------------------------------
\\MAROON
The command completed successfully.
```

Discover Hosts on the same workgroup

Last but not least the **netstat** command can be used with the parameters -n -a -o to display all the active connections along with the IP addresses and process ID of each connection.

```
C:\WINDOWS\system32>netstat -nao
netstat -nao

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       948
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       864
  TCP    0.0.0.0:5800           0.0.0.0:0              LISTENING       1760
  TCP    0.0.0.0:5900           0.0.0.0:0              LISTENING       1760
  TCP    127.0.0.1:1030         0.0.0.0:0              LISTENING       468
  TCP    127.0.0.1:5152         0.0.0.0:0              LISTENING       1644
  TCP    172.16.212.128:139     0.0.0.0:0              LISTENING       4
  TCP    172.16.212.128:1163    172.16.212.1:4444      ESTABLISHED     1048
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    692
  UDP    0.0.0.0:1025           *:*                                    1136
  UDP    0.0.0.0:1026           *:*                                    1136
  UDP    0.0.0.0:4500           *:*                                    692
  UDP    127.0.0.1:123          *:*                                    1048
  UDP    127.0.0.1:1900         *:*                                    1240
  UDP    172.16.212.128:123     *:*                                    1048
  UDP    172.16.212.128:137     *:*                                    4
  UDP    172.16.212.128:138     *:*                                    4
  UDP    172.16.212.128:1900    *:*                                    1240
```

Active Connections

Conclusion

In this article we saw some common commands and their output that can be used for post exploitation activities in Windows networks.The majority of these commands will help us to identify new hosts and network shares which can lead us to compromise further systems on the network.