NetCease Tool

Research Conducted by: Itai Grady, MicrosoftATA[1] Research Team

Written by: Itai Grady, Tal Be'ery, MicrosoftATA Research Team

October 2016

Table of Contents

1 https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

1 Overview

Reconnaissance (recon for short) is a key stage within the Advanced Attackers kill chain. Once attackers have breached a single end-point, they need to discover their next targets within the victim's corporate network, most notably privileged users.

Once attackers had "zoomed in" on target users, they need to find out the computers they had logon to, in order to propagate to them and compromise their credentials. Applying the SMB Session enumeration via the NetSessionEnum method against the DC (or other file servers), allows the attackers to get that information. Recently, some frameworks (e.g. BloodHound[2]) have automated that mapping process.

By default, NetSessionEnum method can be executed by any authenticated user, including network connected users, which effectively means that any domain user is able to execute it remotely.

Since the only current method to modify the default permissions for NetSessionEnum is by manually editing hex registry entry, we wrote the "NetCease" tool, a short PowerShell (PS) script which alters these default permissions. This hardening process should block attackers from easily getting valuable recon information.

2 https://github.com/adaptivethreat/BloodHound

1 Net Session Enumeration

Net Session Enumeration is a method used to retrieve information about established sessions on a server. Any domain user can query a server for its established sessions and get the following information:

- The name/IP address of the computer.
- The name of the user who established the session.
- The number of seconds the session has been active. (since the query)
- The number of seconds the session has been idle. (since the query)

Since all domain users/computers are updating their Group Policy approximately every 90 minutes, they establish a session to the DC and query for an update. Those sessions are visible to all domain users using the NetSessionEnum on that DC.[3]

Several widely-available tools implement such query, including the NetSess tool

```
C:\Research\NetSess>NetSess.exe dc1

NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004

Enumerating Host: dc1
Client                  User Name               Time        Idle Time
------------------------------------------------------------------------------
\\\\192.168.0.10        user1                   000:00:13   000:00:00
\\\\192.168.0.4         CLIENT4-PC$             000:01:11   000:01:00
\\\\[::1]               DC1$                    000:00:02   000:00:02
\\\\192.168.0.4         Administrator           000:00:02   000:00:02

Total of 4 entries enumerated
```

*Figure **1**:NetSess tool result example.*

MicrosoftATA[4] detects the use of such query and alerts the security administrator about it

3https://microsoft.sharepoint.com/teams/Aorato/Shared%20Documents/Research/NTLM/Revealing%20NTLM%20Authenticated%20User%20using%20NetSess.docx?d=weba80c33af934227b2c1c72203baf64c

4 https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

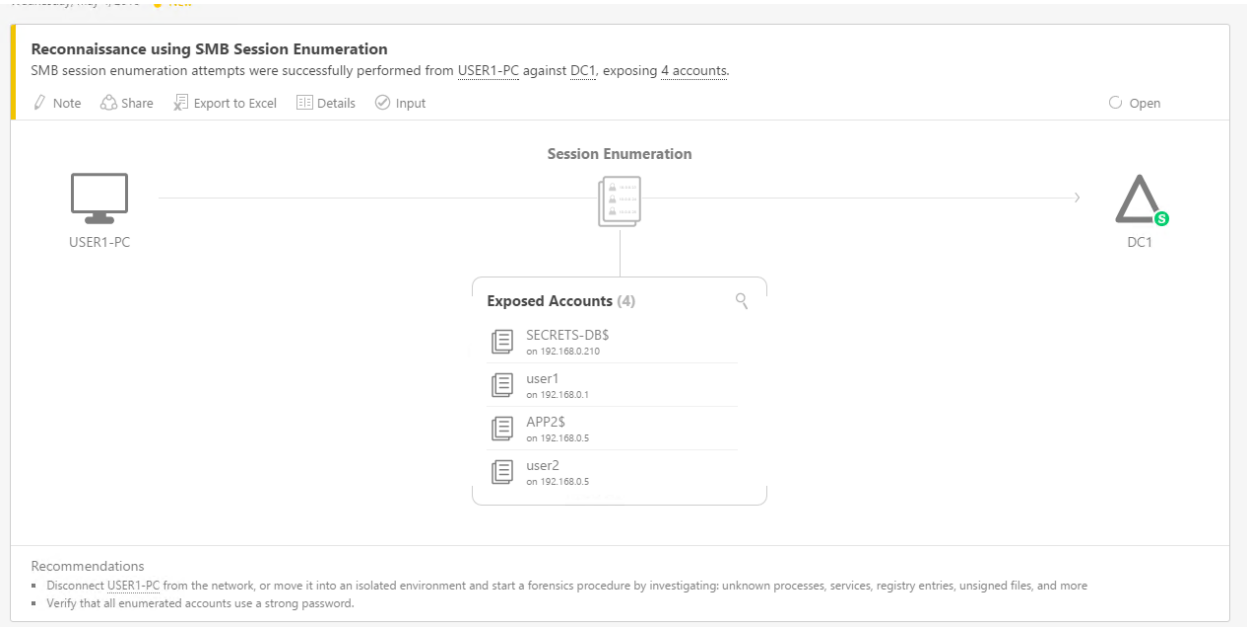

Figure 2 MicrosoftATA alert on NetSessionEnum use

2 NetSessionEnum permissions

NetSessionEnum method permissions are controlled by a registry key under the following path:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/LanmanServer/DefaultSecurity/SrvsvcSessionInfo

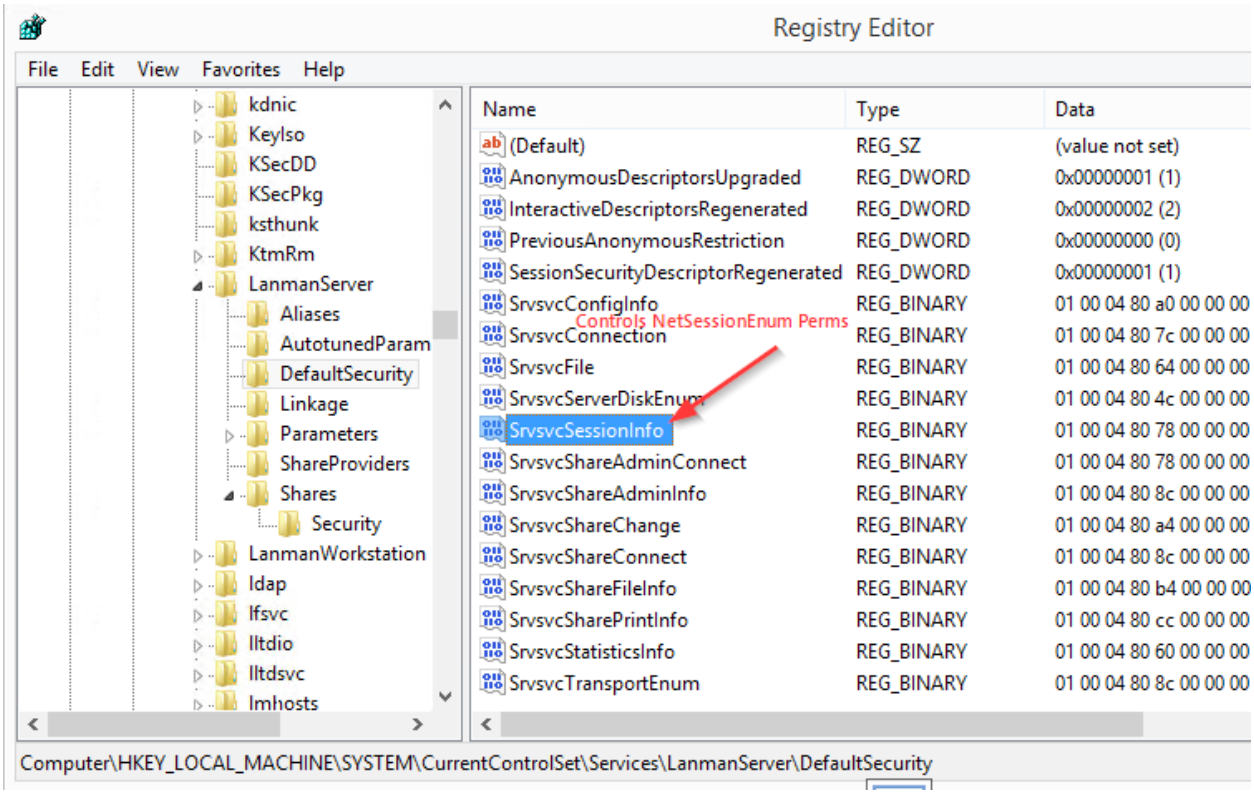

Figure 3 NetSessionEnum DACL in Registry

By default, this binary SrvsvcSessionInfo value is a Discretionary Access Control List (DACL) containing 4 Access Control Entries (ACE) which allows access to any user with at least one of the following characteristics:

- Member of Administrators group (Security Identifier (Sid) S-1-5-32-544)
- Member of Server Operators group (Sid S-1-5-32-549)
- Member of Power Users group (Sid S-1-5-32-547)
- Last but not least Authenticated Users group (Sid S-1-5-11)

By performing a successful network authentication against a domain joined machine, the users (or attackers) obtain the permission to execute NetSessionEnum on that machine, as they got the "Authenticated Users" Sid added to their authentication context.

3 NetCease details

The NetCease script hardens the access to the NetSessionEnum method by removing the execute permission for Authenticated Users group and adding permissions for interactive, service and batch logon sessions.
This will allow any administrator, system operator and power user to remotely call this method, and any interactive/service/batch logon session to call it locally.

Calling NetSess on a hardened machine from remote, using an administrator account:

```
C:\Research\NetSess>whoami
domain1\administrator

C:\Research\NetSess>ipconfig

Windows IP Configuration


Ethernet adapter External:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7844:c6cf:6b6f:be70%13
   IPv4 Address. . . . . . . . . . . : 192.168.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.200

Ethernet adapter Internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{248B11C4-0755-45DB-AFDA-881053CE524B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Research\NetSess>NetSess.exe 192.168.0.4

NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004

Enumerating Host: 192.168.0.4
Client                 User Name                Time        Idle Time
------------------------------------------------------------------------
\\\\192.168.0.10       Administrator            000:00:00   000:00:00

Total of 1 entries enumerated
```

Figure 4:Administrator successfully calls NetSess from remote on a hardened machine

Calling NetSess on a hardened machine from remote, using non privileged user:

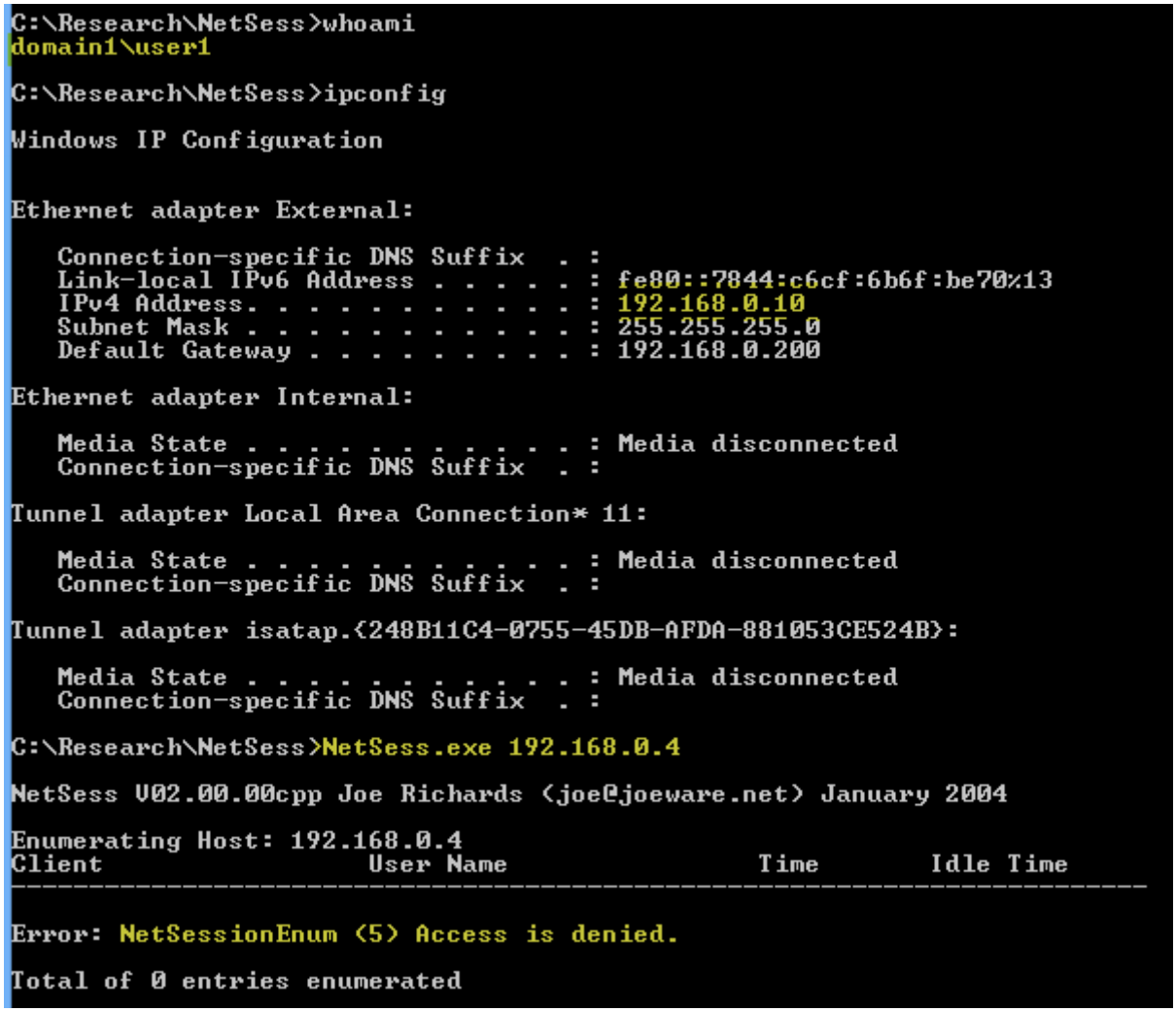

Figure 5:User1 (non-admin) get access denied calling NetSess remotely

Calling NetSess on the same hardened machine, using the same user but locally:

```
C:\Tools\NetSess>whoami
domain1\user1

C:\Tools\NetSess>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4f4:876d:aa5e:55f4%2
   IPv4 Address. . . . . . . . . . . : 192.168.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.200

Ethernet adapter Ethernet 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : corp.microsoft.com

Tunnel adapter isatap.{21A97DB5-6FE0-48D4-A6D9-C7E7C47BD282}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Tools\NetSess>NetSess.exe 192.168.0.4

NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004

Enumerating Host: 192.168.0.4
Client                 User Name               Time       Idle Time
------------------------------------------------------------------------------
\\\\192.168.0.4        user1                   000:00:00  000:00:00

Total of 1 entries enumerated
```

Figure 6:User1 (non-admin) successfully calls NetSess locally

4 Using NetCease.ps1

NetCease is simple to use. Run the PowerShell script as administrator on the machine you wish to harden (DC in most cases). In order for the changes to take effect, restart the "Server" service.

Note that hardening NetSession and hindering attackers' ability to abuse it, does not damage defenders' ability to detect the attack, as MicrosoftATA detects failed recon attempts as well

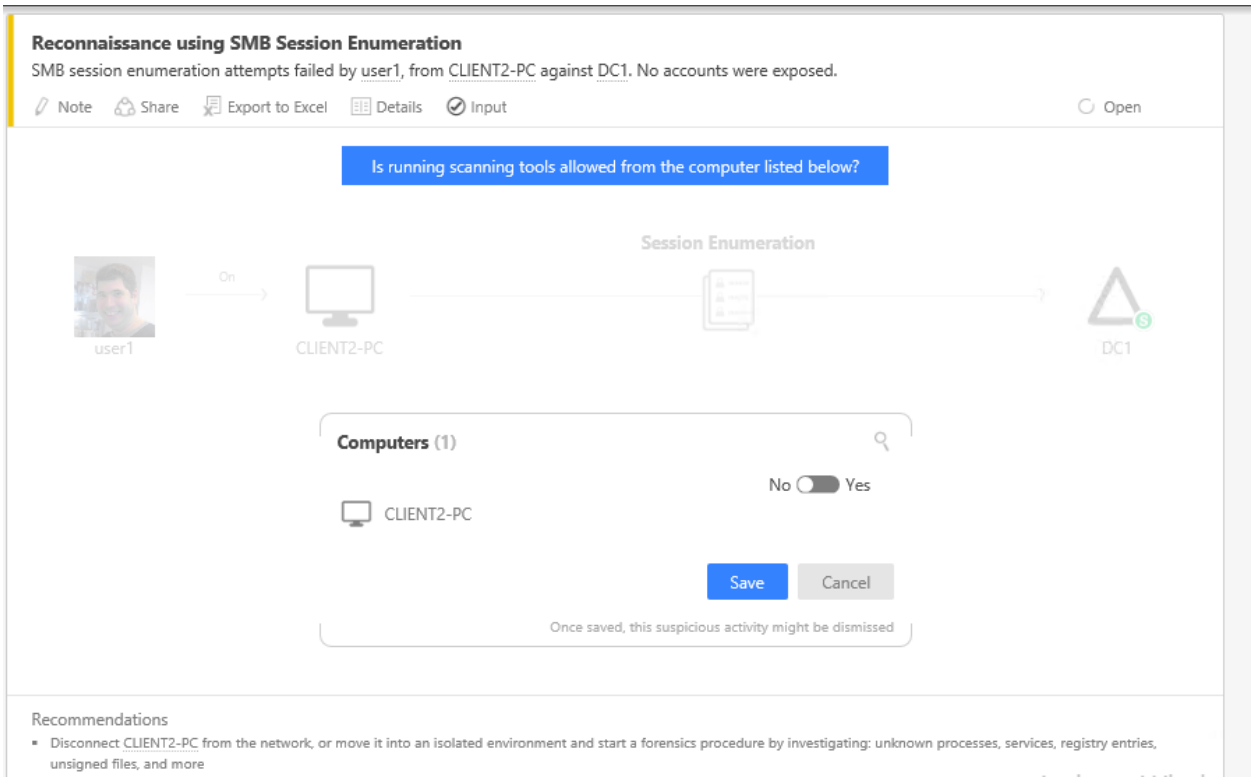

Figure 7 MicrosoftATA detection of a failed NetSessionEnum recon attempt