COMSEC Group
Cyber & Information Security

The forgotten interface: Windows named pipes

Your host

Gil Cohen

CTO, Comsec Global

- IDF Programming course graduate (“Mamram”) and former waterfall developers
- Cyber Security professional with more than 12 years of experience
- Vast comprehensive knowledge in penetration tests, secured design, programmers’ training and information security in general

30 years

Established in 1987, Comsec has nearly three-decades of experience in all aspects of information security.

150 consultants

Allows us to deliver a broad spectrum of services and to provide a uniquely flexible service level.

600 clients

From blue chip companies to start-ups, Comsec has a deep sector expertise in most verticals and un-paralleled understanding of our clients’ business environment.

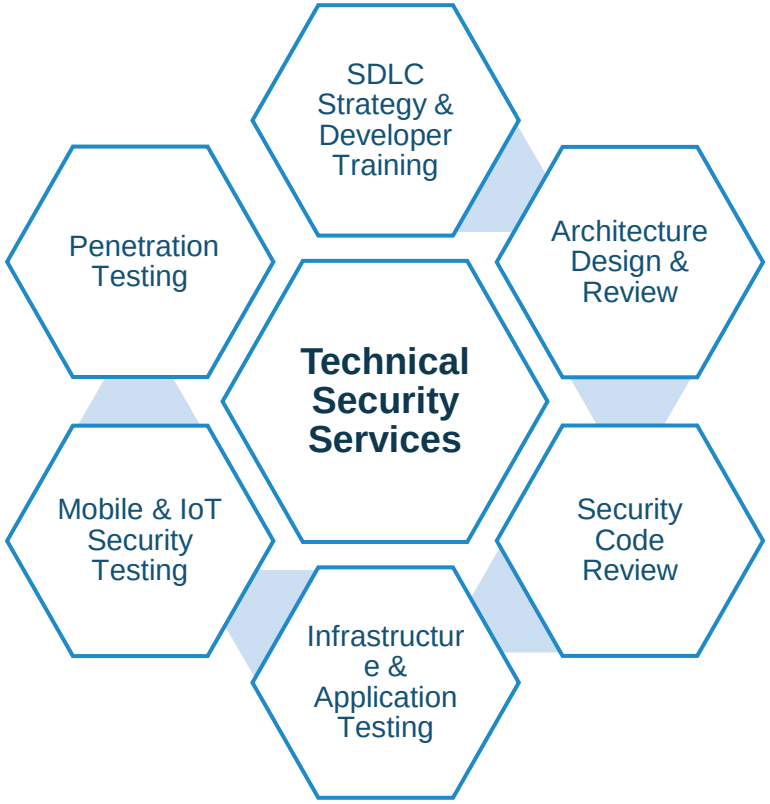
22 countries

With offices in London, Rotterdam and excellence center in Tel Aviv, Comsec is able to deliver global impact through local presence spanning over 22 countries and five continents.

COMSEC Group
Cyber & Information Security

core Services

Innovation, Knowledge & Experience to Keep You Ahead of the Curve.



COMSEC Group
Cyber & Information Security

Key Terms

COMSEC Group
Cyber & Information Security

Introduction To Key Terms

IPC or ***Inter-Process Communication***

- An operating system mechanism that allows **processes** and **applications** to manage **shared data** and **communicate**
- Categorized as **clients** and **servers**, where the client requests data and the server responds to client requests
- Many applications are **both clients and servers**, as commonly seen in distributed computing

Introduction To Key Terms

Windows Named Pipes

- One of the methods to perform ***IPC*** in ***Microsoft Windows***
- **One-way** or **duplex** pipe for communication between the **pipe server** and **one or more pipe clients**
- Utilizes a unique file system called **NPFS**(Named Pipe Filesystem)
- **Any process** can **access** named pipes, subject to **security** checks
- **All instances** of a named pipe share **the same pipe name**, but each instance has its own buffers and handles

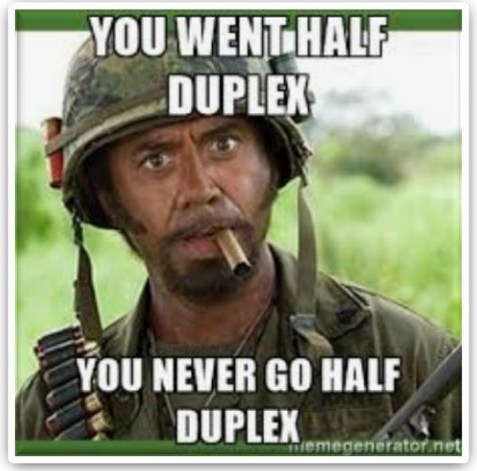
Introduction To Key Terms

Windows Named Pipes

Many configurations and variations:

- Half Duplex or Full Duplex.
- Byte-Oriented or Packet-Oriented.
- Local or **Network**.

Inter-process communication is not only local!



Named pipes network communication is **not encrypted** and uses the protocols **SMB (port 445) or DCE\RPC (port 135)**

COMSEC Group
Cyber & Information Security

Introduction To Key Terms

RPC or ***R****emote* ***P****rocedure* ***C****all*

- A protocol that allows one program to invoke a service from a program located on another computer

- No need to understand the network's structure\details

- Uses port 135 TCP or UDP

DCE/RPC *or* ***D****istributed* ***C****omputing* ***E****nvironment /* ***R****emote* ***P****rocedure* ***C****alls*

- A facility for calling a procedure on a remote as if it were a local procedure call

- To the programmer, a remote call looks like a local call

Introduction To Key Terms

SMB* or *Server Message Block

- An application-layer network protocol providing shared access to files, printers, serial ports etc.

- Mostly used for file sharing
  \\192.168.1.1\c$\Users\manager\Documents
  \\fileserver\public\shareddocs

- Also provides an authenticated inter-process communication mechanism

- Uses port number 445 TCP

SMB in a nutshell

COMSEC Group
Cyber & Information Security

Introduction To Key Terms

Named and Unnamed \ anonymous Pipes

Two types of named pipes:

- ***Named pipes***: has a specific name, all instances share the name

- ***Unnamed \ anonymous pipe***: is not given a name
  - Only used for communication between a **child** and it's **parent process**
  - Always local; they **cannot be used** for **communication** over a network
  - **Vanishes** as soon as it is **closed**, or one of the process (parent or child) completes execution
  - Actually named pipes with a **random name**

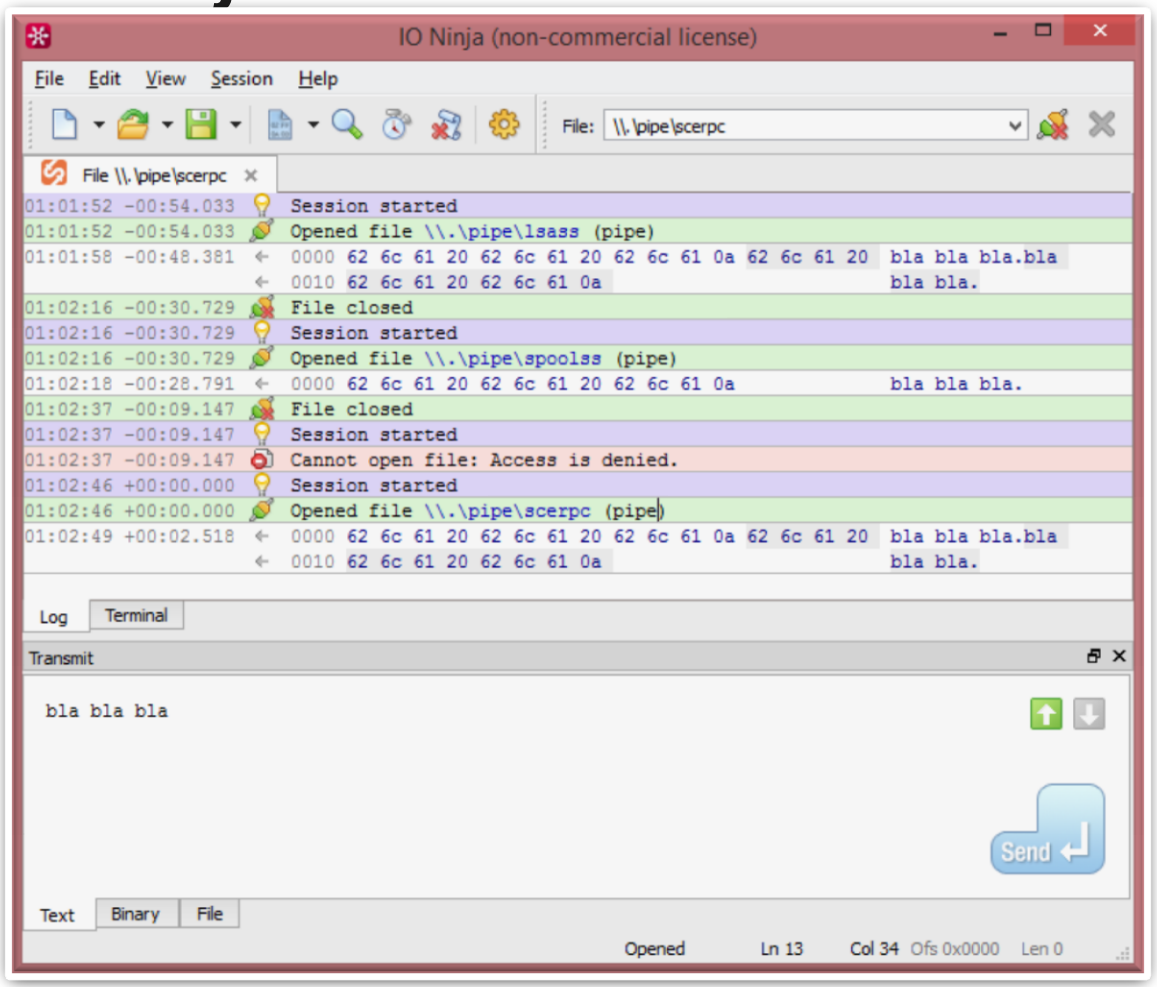
Connecting To A Named Pipe

Connecting To A Named Pipe

- All pipes placed in the root directory of NPFS
- **Cannot** be mounted within the **normal filesystem**
- Mounted under the special path - **\\.\pipe\{pipe name}**
  - A pipe named "foo" would have a full path name of: **\\.\pipe\foo**
  - Remote connection: **\\10.0.0.1\pipe\foo**
- Can be connected to programmatically or with dedicated tools

Connecting To A Named Pipe

IO Ninja



- Named pipes (and other communications) Swiss army knife
- http://tibbo.com/ninja.htm
- Free for non-commercial usage ☺

COMSEC Group
Cyber & Information Security

Pipe ACLs And Connection Limitation

COMSEC Group
Cyber & Information Security

Pipe ACLs And Connection Limitation

- Named pipes are implemented by a filesystem driver in Windows NT, npfs.sys, which supports **security descriptors**
- Security descriptors are used to **control access** to named pipes.
- By default **DACL** (Discretionary Access Control Lists) permissions are set to **everyone** using **anonymous login** (null sessions)
- ACLs can be modified to allow only specific users (same as file ACLs)

Pipe ACLs And Connection Limitation

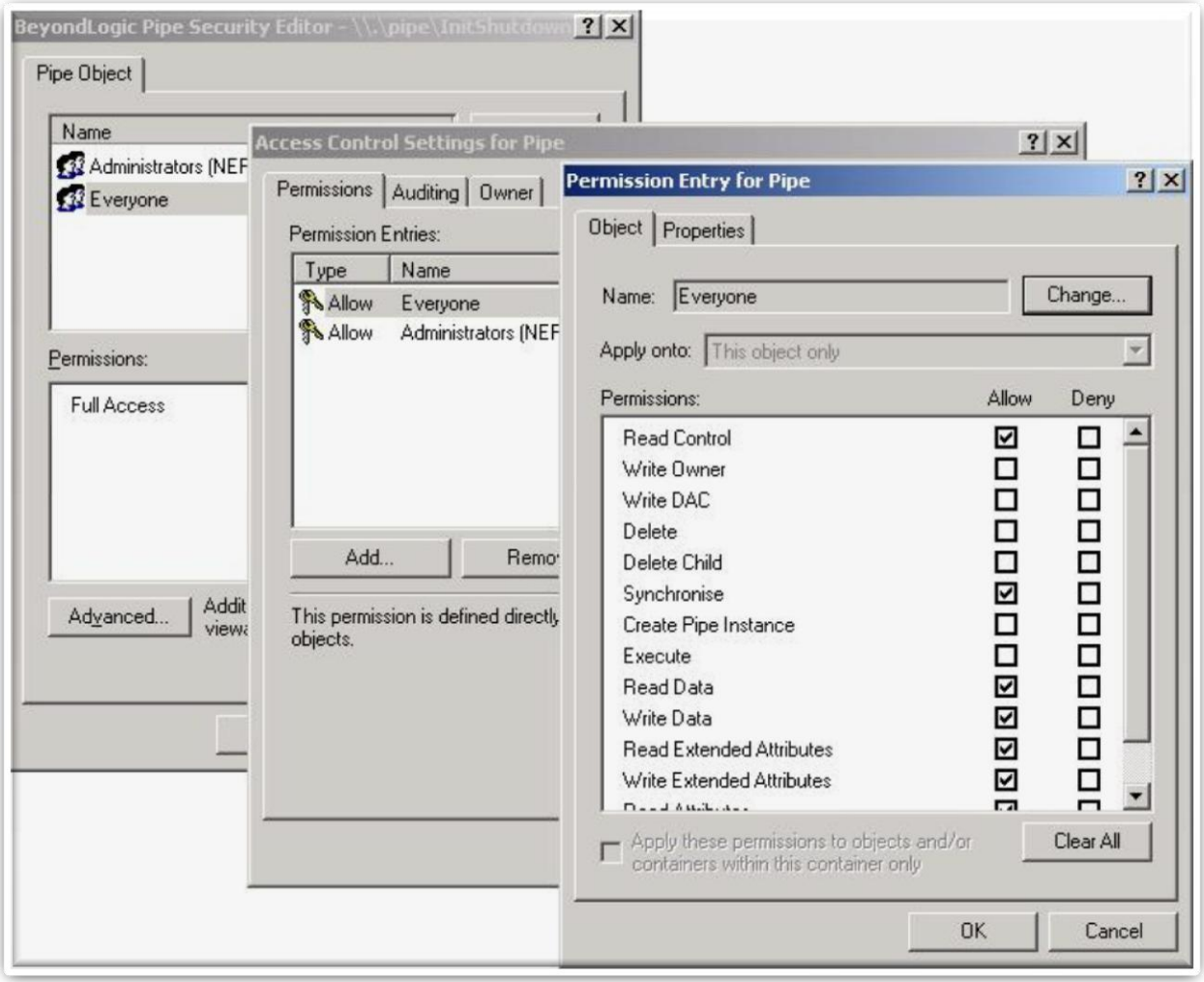
Named Pipes have Access Control Lists.
For the following pipe it is permitted to everyone to connect:

```
G:\Network\Named Pipes>pipeacl \??\pipe\initshutdown
Revision: 1
Reserved: 0
Control : 8004
Owner: BUILTIN\Administrators (S-1-5-32-544)
Group: SYSTEM (S-1-5-18)
Sacl: Not present
Dacl: 3 aces
(A) (00) 0012019b :      Everyone (S-1-1-0)
(A) (00) 0012019b :      Anonymous (S-1-5-7)
(A) (00) 001f01ff :      BUILTIN\Administrators (S-1-5-32-544)
```

Pipe ACLs And Connection Limitation

Named pipes ACLs enumeration

- **Using other 3rd party tools**
- **For example: Beyond Security Pipe Security Editor**



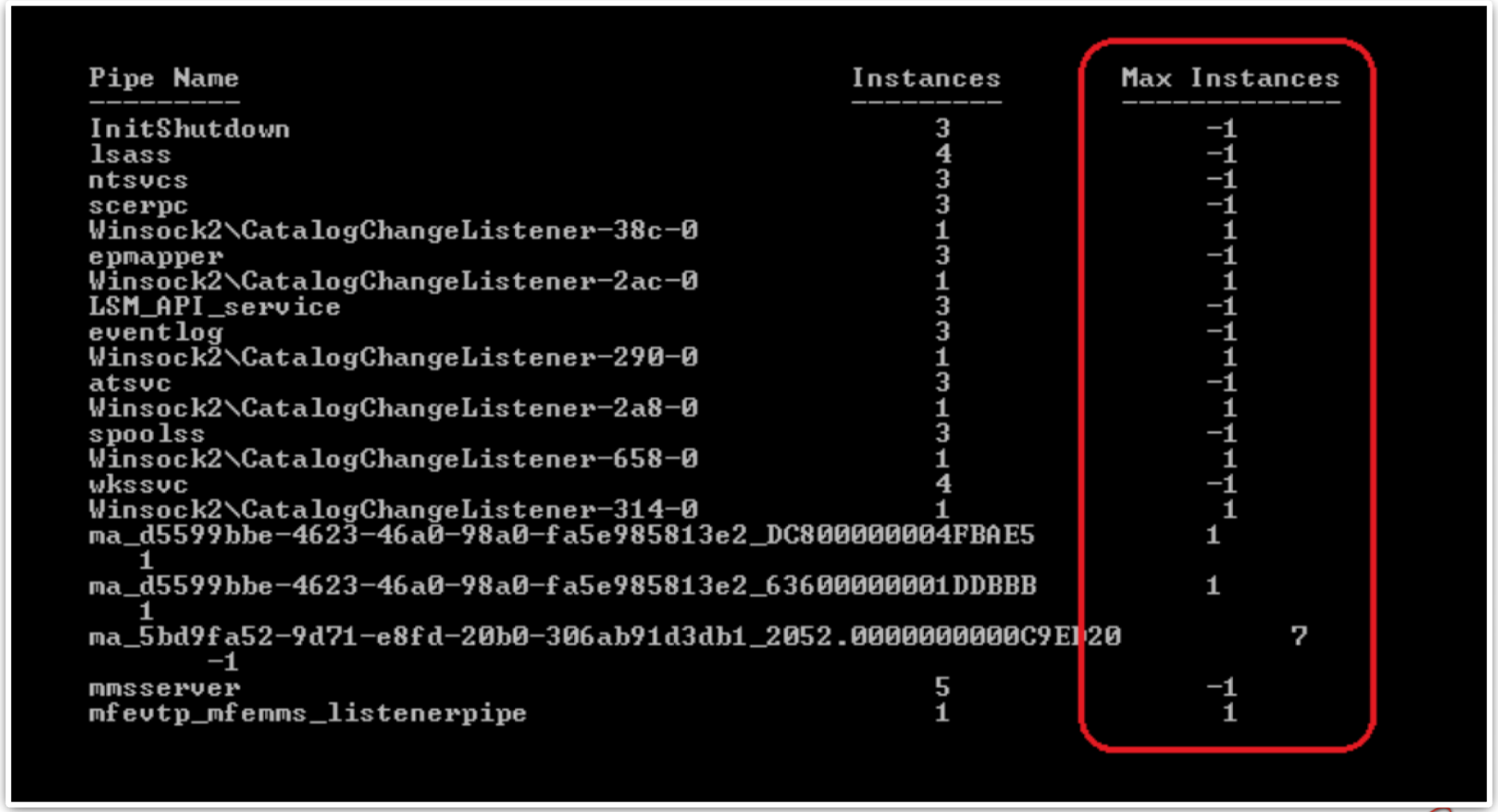
An old utility, deprecated

Win32 Pipe Security Editor
for Windows NT/2000/XP
http://retired.beyondlogic.org/solutions/pipesec/pipesec.htm

COMSEC Group
Cyber & Information Security

Pipe ACLs And Connection Limitation

Another limitation of Windows Named Pipes in the **max number of instances** of a pipe



Pipe Name	Instances	Max Instances
InitShutdown	3	-1
lsass	4	-1
ntsvcs	3	-1
scerpc	3	-1
Winsock2\CatalogChangeListener-38c-0	1	1
epmapper	3	-1
Winsock2\CatalogChangeListener-2ac-0	1	1
LSM_API_service	3	-1
eventlog	3	-1
Winsock2\CatalogChangeListener-290-0	1	1
atsvc	3	-1
Winsock2\CatalogChangeListener-2a8-0	1	1
spoolss	3	-1
Winsock2\CatalogChangeListener-658-0	1	1
wkssvc	4	-1
Winsock2\CatalogChangeListener-314-0	1	1
ma_d5599bbe-4623-46a0-98a0-fa5e985813e2_DC800000004FBAE5	1	1
ma_d5599bbe-4623-46a0-98a0-fa5e985813e2_63600000001DDBBB	1	1
ma_5bd9fa52-9d71-e8fd-20b0-306ab91d3db1_2052.0000000000C9E	20	7
mmsserver	5	-1
mfevtp_mfemms_listenerpipe	1	1

Enumerating And Scanning For Named Pipes

COMSEC Group
Cyber & Information Security

Enumerating And Scanning For Named Pipes

Named pipes can be enumerated using different testing tools.

For locally detecting which named pipes are opened, it is possible to use Sysinternals' **pipelist**:

```
C:\Users\                                \Named Pipes\Tools\Scripts>pipeli
xe

PipeList v1.02 - Lists open named pipes
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Pipe Name                                          Instances       Max Instances
---------                                          ---------       -------------
InitShutdown                                               3                  -1
lsass                                                      4                  -1
ntsvcs                                                     3                  -1
scerpc                                                     3                  -1
Winsock2\CatalogChangeListener-3a0-0                       1                   1
epmapper                                                   3                  -1
Winsock2\CatalogChangeListener-2b4-0                       1                   1
LSM_API_service                                            3                  -1
eventlog                                                   3                  -1
Winsock2\CatalogChangeListener-1d8-0                       1                   1
{14579667-532A-42C2-9200-FD0544E09B90}                     1                   1
{18837DD8-C4DF-4E48-8CB6-3DD8E59C2DD5}                     1                   1
Winsock2\CatalogChangeListener-2fc-0                       1                   1
atsvc                                                      3                  -1
Winsock2\CatalogChangeListener-210-0                       1                   1
spoolss                                                    3                  -1
Winsock2\CatalogChangeListener-694-0                       1                   1
wkssvc                                                     4                  -1
ma_d5599bbe-4623-46a0-98a0-fa5e985813e2_2486600000001172                      1
```

https://download.sysinternals.com/files/PipeList.zip

COMSEC Group
Cyber & Information Security

Enumerating And Scanning For Named Pipes

Named pipes ACLs enumeration

using SysInternals' pipeacl

- enables viewing permission of a certain named pipes:

```
C:\> pipeacl \.\pipe\lsarpc

Revision: 1
Reserved: 0
Control : 8004
Owner: BUILTIN\Administrators (S-1-5-32-544)
Group: SYSTEM (S-1-5-18)
Sacl: Not present
Dacl: 3 aces
(A) (00) 001f01ff :     BUILTIN\Administrators (S-1-5-32-544)
(A) (00) 0012019b :     Anonymous (S-1-5-7)
(A) (00) 0012019b :     Everyone (S-1-1-0)
```

www.securityfocus.com/tools/2629

Enumerating And Scanning For Named Pipes

Forgotten Metasploit module called **Pipe auditor** enumerate **remotely** accessible named pipes, over SMB (**Pipe_Auditor**) or RPC (**Pipe_dcerpc_auditor)**

```
msf auxiliary(pipe_auditor) > use auxiliary/scanner/smb/pipe_dcerpc_auditor
msf auxiliary(pipe_dcerpc_auditor) > set RHOSTS 192.168.10.60-110
RHOSTS => 192.168.10.60-110
msf auxiliary(pipe_dcerpc_auditor) > set THREADS 11
THREADS => 11
msf auxiliary(pipe_dcerpc_auditor) > show options

Module options (auxiliary/scanner/smb/pipe_dcerpc_auditor):

   Name       Current Setting    Required  Description
   ----       ---------------    --------  -----------
   RHOSTS     192.168.10.60-110  yes       The target address range or CIDR identifier
   SMBDomain  WORKGROUP          no        The Windows domain to use for authentication
   SMBPIPE    BROWSER            yes       The pipe name to use (BROWSER)
   SMBPass                       no        The password for the specified username
   SMBUser                       no        The username to authenticate as
   THREADS    11                 yes       The number of concurrent threads

msf auxiliary(pipe_dcerpc_auditor) >
```

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/pipe_auditor.rb

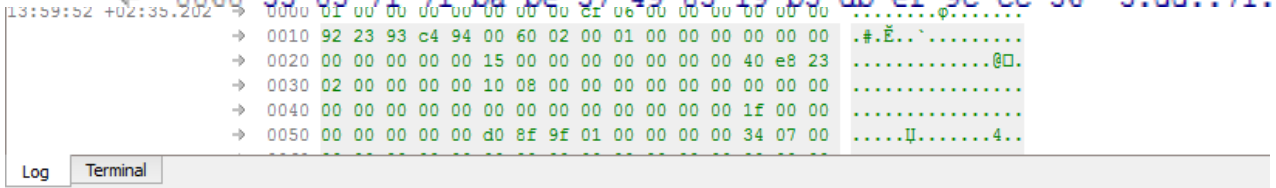
Sniffing Named Pipes Content

Sniffing Named Pipes Content

IO Ninja also enables sniffing and monitoring traffic of a chosen named pipe:

http://tibbo.com/ninja.html

```
13:57:18 +00:01.540   File #1: Client file opened: \wkssvc
13:57:18 +00:01.540 ← 0000 05 00 0b 03 10 00 00 00 74 00 00 00 02 00 00 00  ........t.......
                    ← 0010 b8 10 b8 10 00 00 00 00 02 00 00 00 00 00 01 00  ................
                    ← 0020 98 d0 ff 6b 12 a1 10 36 98 33 46 c3 f8 7e 34 5a  .п.k...6.3Fø.~4Z
                    ← 0030 01 00 00 00 04 5d 88 8a eb 1c c9 11 9f e8 08 00  .....]..□....□..
                    ← 0040 2b 10 48 60 02 00 00 00 01 00 01 00 98 d0 ff 6b  +.H`.........п.k
                    ← 0050 12 a1 10 36 98 33 46 c3 f8 7e 34 5a 01 00 00 00  ...6.3Fø.~4Z....
                    ← 0060 2c 1c b7 6c 12 98 40 45 03 00 00 00 00 00 00 00  ,..l..@E........
                    ← 0070 01 00 00 00                                      ....
13:57:18 +00:01.540 → 0000 05 00 0c 03 10 00 00 00 5c 00 00 00 02 00 00 00  ........\.......
                    → 0010 b8 10 b8 10 7e 3b 00 00 0d 00 5c 50 49 50 45 5c  ....~;....\PIPE\
                    → 0020 77 6b 73 73 76 63 00 00 02 00 00 00 00 00 00 00  wkssvc..........
                    → 0030 04 5d 88 8a eb 1c c9 11 9f e8 08 00 2b 10 48 60  .]..□....□..+.H`
                    → 0040 02 00 00 00 03 00 03 00 00 00 00 00 00 00 00 00  ................
                    → 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ..............
13:57:23 +00:06.508   File #2: Client file opened: \wkssvc
13:57:23 +00:06.509 ← 0000 05 00 0b 03 10 00 00 00 a0 00 00 00 02 00 00 00  ................
                    ← 0010 b8 10 b8 10 00 00 00 00 03 00 00 00 00 00 01 00  ................
                    ← 0020 98 d0 ff 6b 12 a1 10 36 98 33 46 c3 f8 7e 34 5a  .п.k...6.3Fø.~4Z
                    ← 0030 01 00 00 00 04 5d 88 8a eb 1c c9 11 9f e8 08 00  .....]..□....□..
                    ← 0040 2b 10 48 60 02 00 00 00 01 00 01 00 98 d0 ff 6b  +.H`.........п.k
                    ← 0050 12 a1 10 36 98 33 46 c3 f8 7e 34 5a 01 00 00 00  ...6.3Fø.~4Z....
                    ← 0060 33 05 71 71 ba be 37 49 83 19 b5 db ef 9c cc 36  3.qq..7I.....ì...
```



COMSEC Group
Cyber & Information Security

Fuzzing Named Pipes

COMSEC Group
Cyber & Information Security

Fuzzing

- **Fuzzing** or **fuzz testing** is an **automated software testing** technique that involves providing **invalid, unexpected, or random data** as inputs to a computer program.
- Done with **fuzzers** – automatic fuzzing tools
- The program is then **monitored** for exceptions such as crashes and potential RCEs.
- Typically, fuzzers are used to test programs that take structured inputs.

Fuzzing

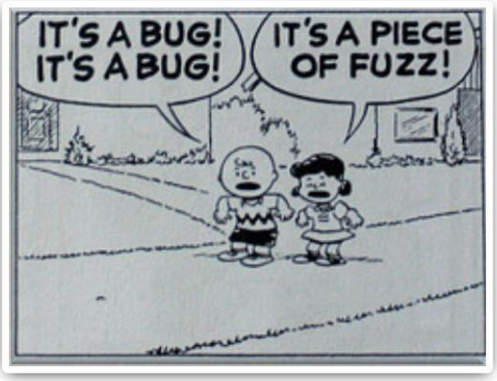
Two types of fuzzing approaches:

Dumb (“Black Box”)

- Go over all possible inputs without understanding the expected ones (sometimes implemented using random data)
- Simple to implement, sometimes impossible to execute using the sequential approach

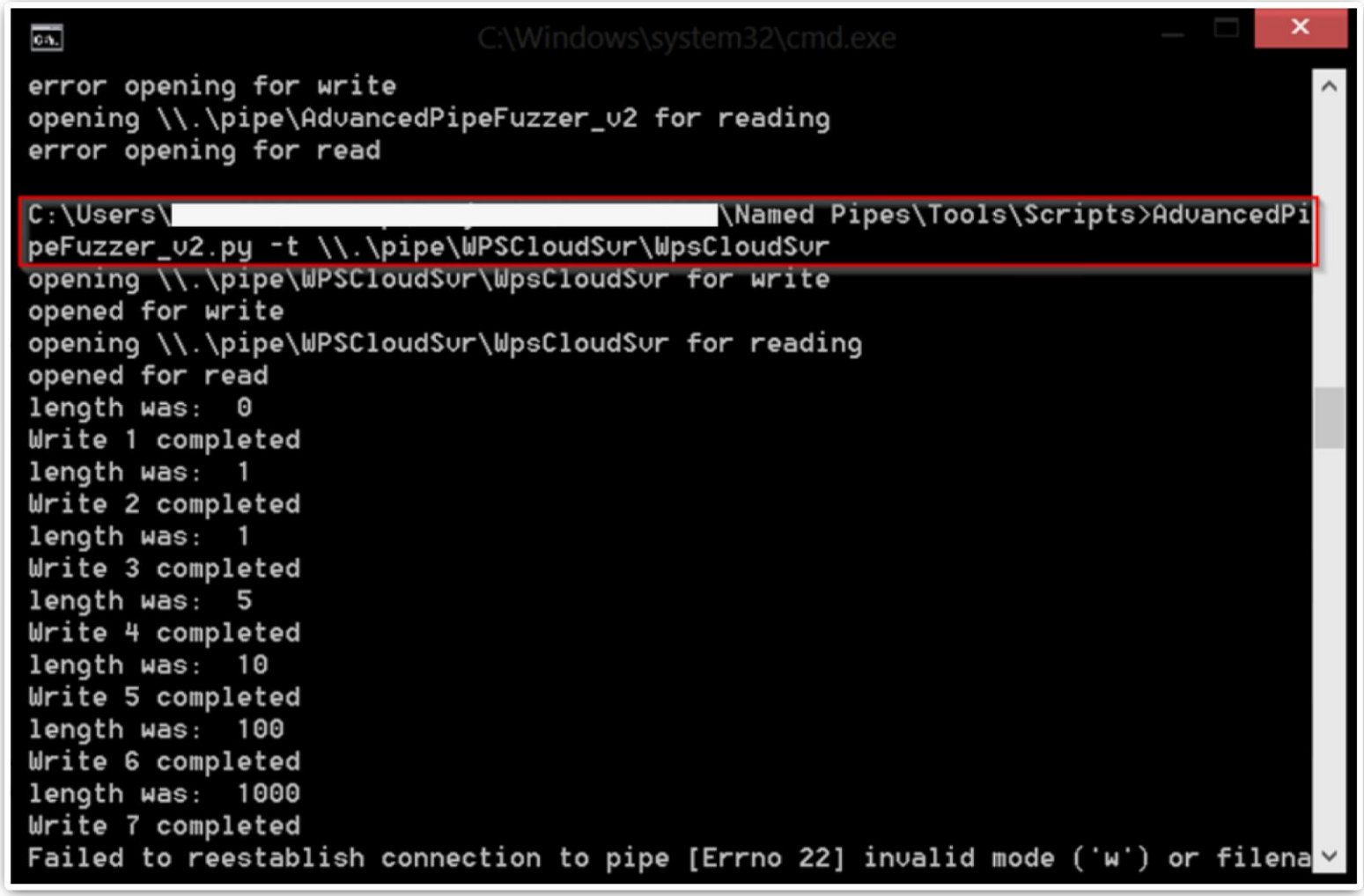
Smart (“White Box”)

- Understand the expected input and fuzz along the edges (mix expected data template with random values)
  – Smart data generation
- Harder to implement, more code coverage



Fuzzing Named Pipes

Windows IPC Fuzzing - dump-fuzzing named pipes script



https://www.nccgroup.trust/us/about-us/resources/windows-ipc-fuzzing-tools/

COMSEC Group
Cyber & Information Security

Exploitation And Impact

COMSEC Group
Cyber & Information Security

Exploitation And Impact

- Many pieces of software work with **hidden** and\or **undocumented APIs**
- The **forgotten nature** of named pipes leave an **uncharted territory** of **socket-like interfaces** that can **contain vulnerabilities**
- If software reads data from the named pipe without any validation of the content, the attacker might trigger **Buffer Overflow** leading to ***Denial of Service*** of the software and even ***Remote Code Execution***

Exploitation And Impact

- If named pipe ACLs allow remote access, **remote DoS or RCE** can be triggered
- Research of the cause behind the crash will allow the attacker to facilitate it as a **zero day vulnerability**
- Could be used to spread a malware in an internal network, as recently seen in the WannaCry ransomware campaign

GAME OVER

COMSEC Group
Cyber & Information Security

Case study: qBittorrent & SugarSync

COMSEC Group
Cyber & Information Security

qBittorrent & SugarSync case study

qBittorrent

- a cross-platform client for the BitTorrent protocol
- Free and open-source, released under the GPLv2
- Written in C++

SugarSync

- A cloud service that enables active synchronization of files across computers and other devices
- Used for file backup, access, syncing, and sharing
- Supports variety of operating systems, such as Android, iOS, Mac OS X, and Windows devices

Exploitation And Impact

Both application use **QT framework**:

- A cross-platform application development framework for desktop, embedded and mobile. Supports multiple platforms and operating systems

- Both applications use the **qtsingleapp** functionality which is responsible for writing temp files

- By **fuzzing** the named pipe both locally and remotely, we managed to **remotely crash the programs**

SugarSync

COMSEC Group
Cyber & Information Security

Demo

Mitigation And Defense

Mitigation And Defense

Developers point of view

Know the risk!

- When creating a named pipe, set a secured ACL to allow only authorized connections to the named pipes

- Follow the **least privilege** approach
  - Giving a user account only those privileges which are essential to perform its intended function

- If possible, limit the maximum number of instances of a named pipe, thus effectively limiting the number of simultaneous connections

Mitigation And Defense

Users\3rd party software clients point of view

Know the risk!

- Block all unnecessary SMB and RPC services (ports 135 and 445), especially over WAN/Internet
- Segment the network according to security best practices
- Always install the latest software security patches

COMSEC Group
Cyber & Information Security

Mitigation And Defense

Hackers' point of view

Know the opportunity!

- Well… Hack
- Explore remotely accessible named pipes and test for RCE and DoS whenever seeing open SMB or RPC ports
- Have fun! ☺

COMSEC Group
Cyber & Information Security

Closing remarks

- Windows named pipes are a forgotten, remotely accessible, socket-like interface
- A whole, newly rediscovered, potential world of local and remote vulnerabilities – increased attack surface
- Don’t ignore named pipes in Windows desktop applications

Stay safe

Thank you

Gil Cohen

twitter.com/Gilco83
www.linkedin.com/in/gilc83

Gilc@comsecglobal.com

www.comsecglobal.com

Gr33tz & Th2nkz:
Aviad Golan @AviadGolan, linkedin.com/in/aviadgolan
Peter Savranskiy - peters@comsecglobal.com
Reuvein Vinokurov - reuveinv@comsecglobal.com
Coral Benita - coralb@comsecglobal.com
Meareg Hunegnaw - mearegh@comsecglobal.com
Roni Fenergi - ronif@comsecglobal.com
Sharon Ohayon - sharono@comsecglobal.com
Josh Grossman - joshg@comsecglobal.com

COMSEC Group
Cyber & Information Security