COMSEC Group
Cyber & Information Security

Call the plumber –
You have a leak in your (named) pipe

Agenda

- Presenter introduction
- Key terms
- Connecting to named pipes
- Pipe ACLs And Connection Limitation
- Named pipes in the wild
- Enumerating And Scanning For Named Pipes
- Sniffing Named Pipes Content
- Fuzzing Named Pipes
- Exploitation And Impact
- Case studies & Live demo!
- Mitigation And Defense

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

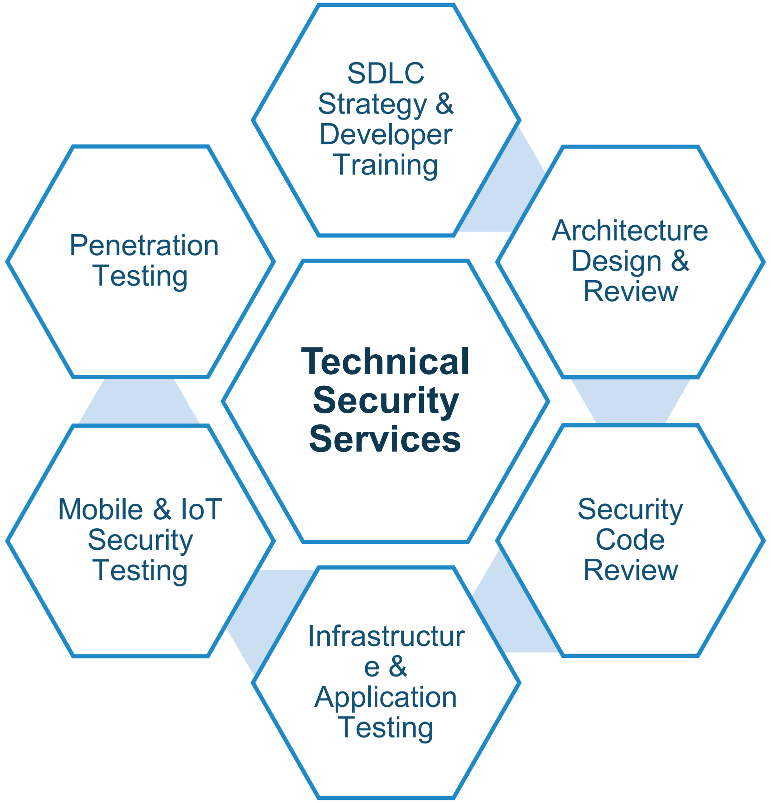
With offices in London, Rotterdam and excellence center in Tel Aviv, Comsec is able to deliver global impact through local presence spanning over 22 countries and five continents.

DEFCON

COMSEC Group
Cyber & Information Security

core Services

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



Technical Security Services

SDLC Strategy & Developer Training

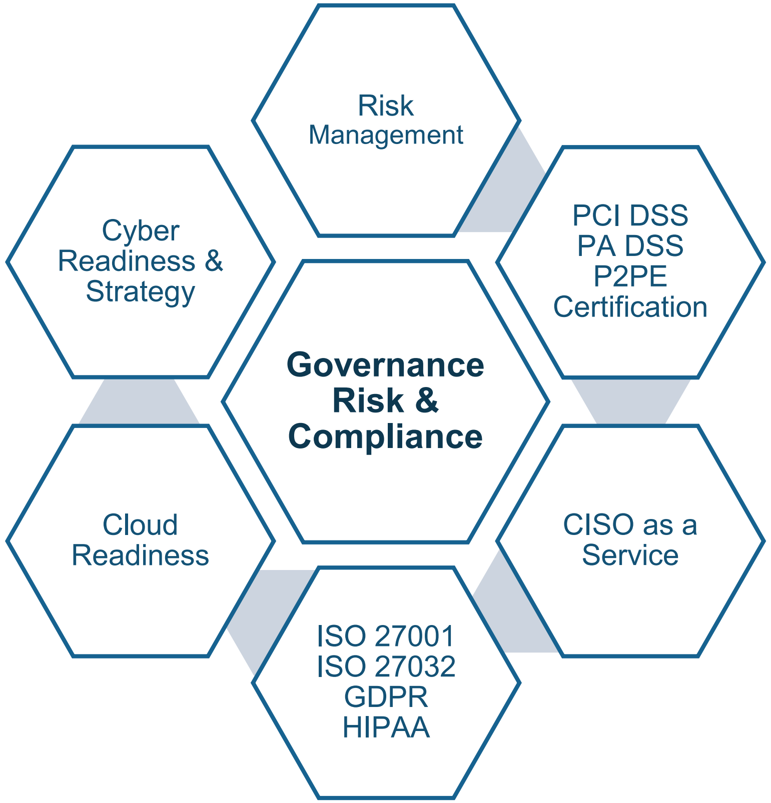
Architecture Design & Review

Security Code Review

Infrastructur e & Application Testing

Mobile & IoT Security Testing

Penetration Testing



Governance Risk & Compliance

Risk Management

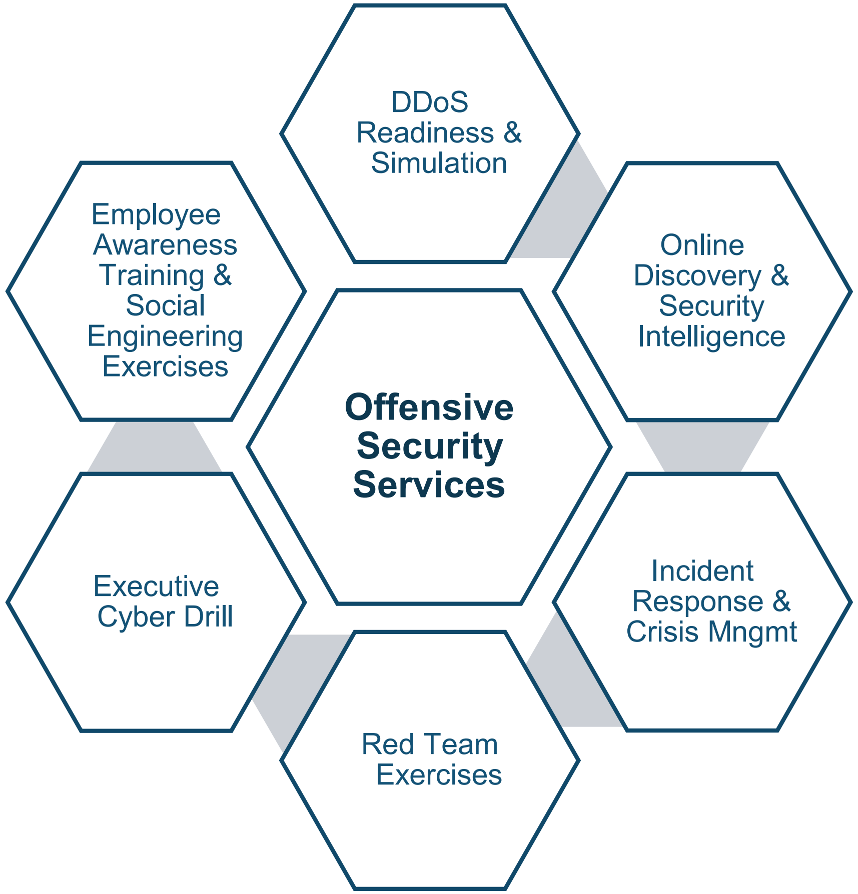
PCI DSS
PA DSS
P2PE
Certification

CISO as a Service

ISO 27001
ISO 27032
GDPR
HIPAA

Cloud Readiness

Cyber Readiness & Strategy



Offensive Security Services

DDoS Readiness & Simulation

Online Discovery & Security Intelligence

Incident Response & Crisis Mngmt

Red Team Exercises

Executive Cyber Drill

Employee Awareness Training & Social Engineering Exercises

Key Terms

COMSEC Group
Cyber & Information Security

Introduction To Key Terms

IPC or ***I**nter-**P**rocess **C**ommunication*

- 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

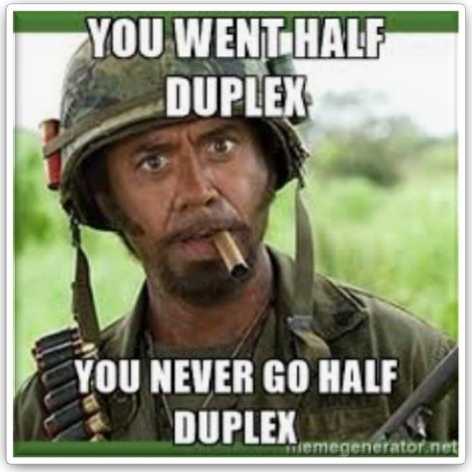
Windows Named Pipes

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)**



DEFCON

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

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

COMSEC Group
Cyber & Information Security

Connecting To A Named Pipe

- All pipes placed in the root directory of NPFS

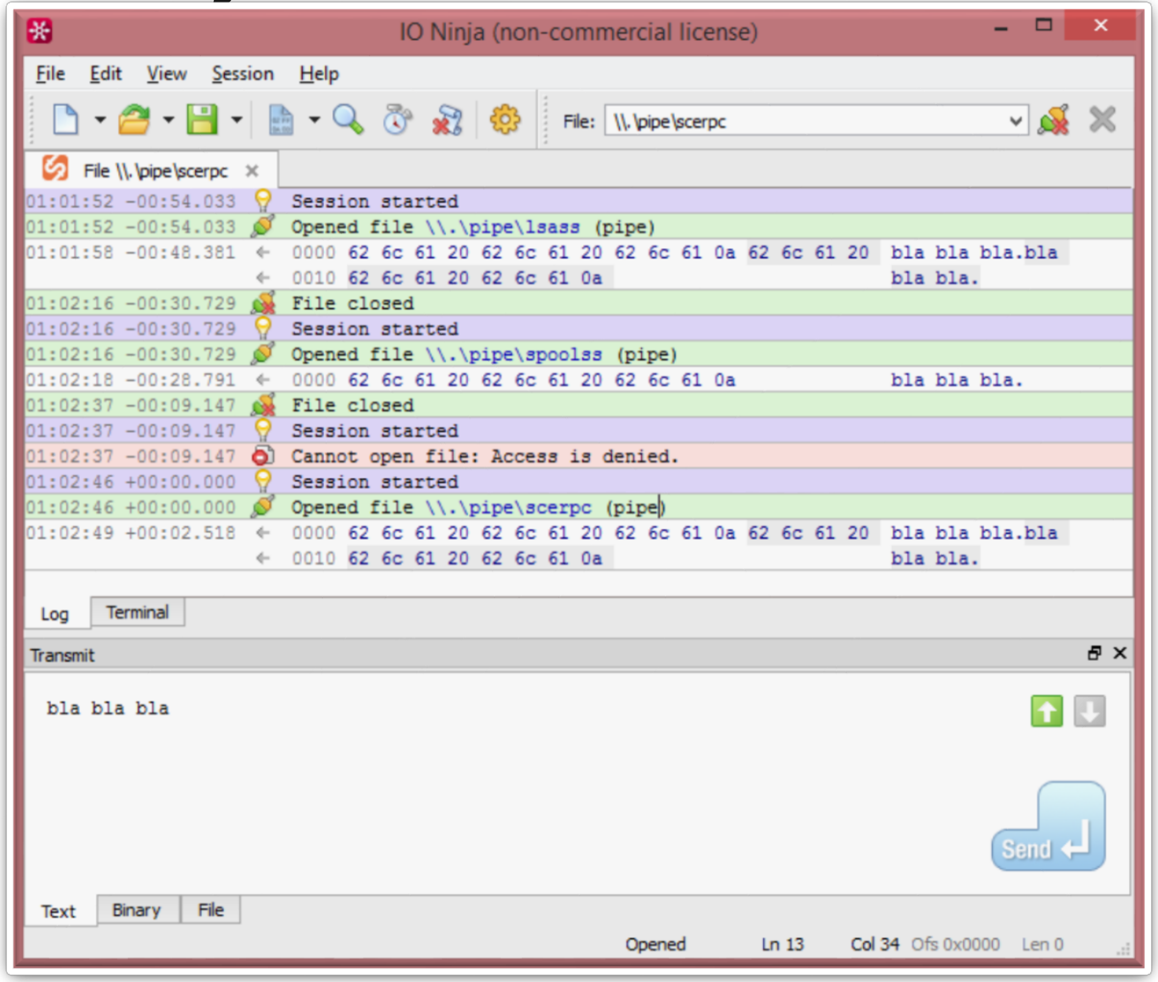
- **Cannot** be mounted within the **normal filesystem**

- 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



```
01:01:52 -00:54.033   Session started
01:01:52 -00:54.033   Opened file \\.\pipe\lsass (pipe)
01:01:58 -00:48.381 ← 0000 62 6c 61 20 62 6c 61 20 62 6c 61 0a 62 6c 61 20  bla bla bla.bla
                    ← 0010 62 6c 61 20 62 6c 61 0a                          bla bla.
01:02:16 -00:30.729   File closed
01:02:16 -00:30.729   Session started
01:02:16 -00:30.729   Opened file \\.\pipe\spoolss (pipe)
01:02:18 -00:28.791 ← 0000 62 6c 61 20 62 6c 61 20 62 6c 61 0a              bla bla bla.
01:02:37 -00:09.147   File closed
01:02:37 -00:09.147   Session started
01:02:37 -00:09.147   Cannot open file: Access is denied.
01:02:46 +00:00.000   Session started
01:02:46 +00:00.000   Opened file \\.\pipe\scerpc (pipe)
01:02:49 +00:02.518 ← 0000 62 6c 61 20 62 6c 61 20 62 6c 61 0a 62 6c 61 20  bla bla bla.bla
                    ← 0010 62 6c 61 20 62 6c 61 0a                          bla bla.
```

```
bla bla bla
```

Opened   Ln 13   Col 34   Ofs 0x0000   Len 0

- Named pipes (and other communications) Swiss army knife

- http://tibbo.com/ninja.htm

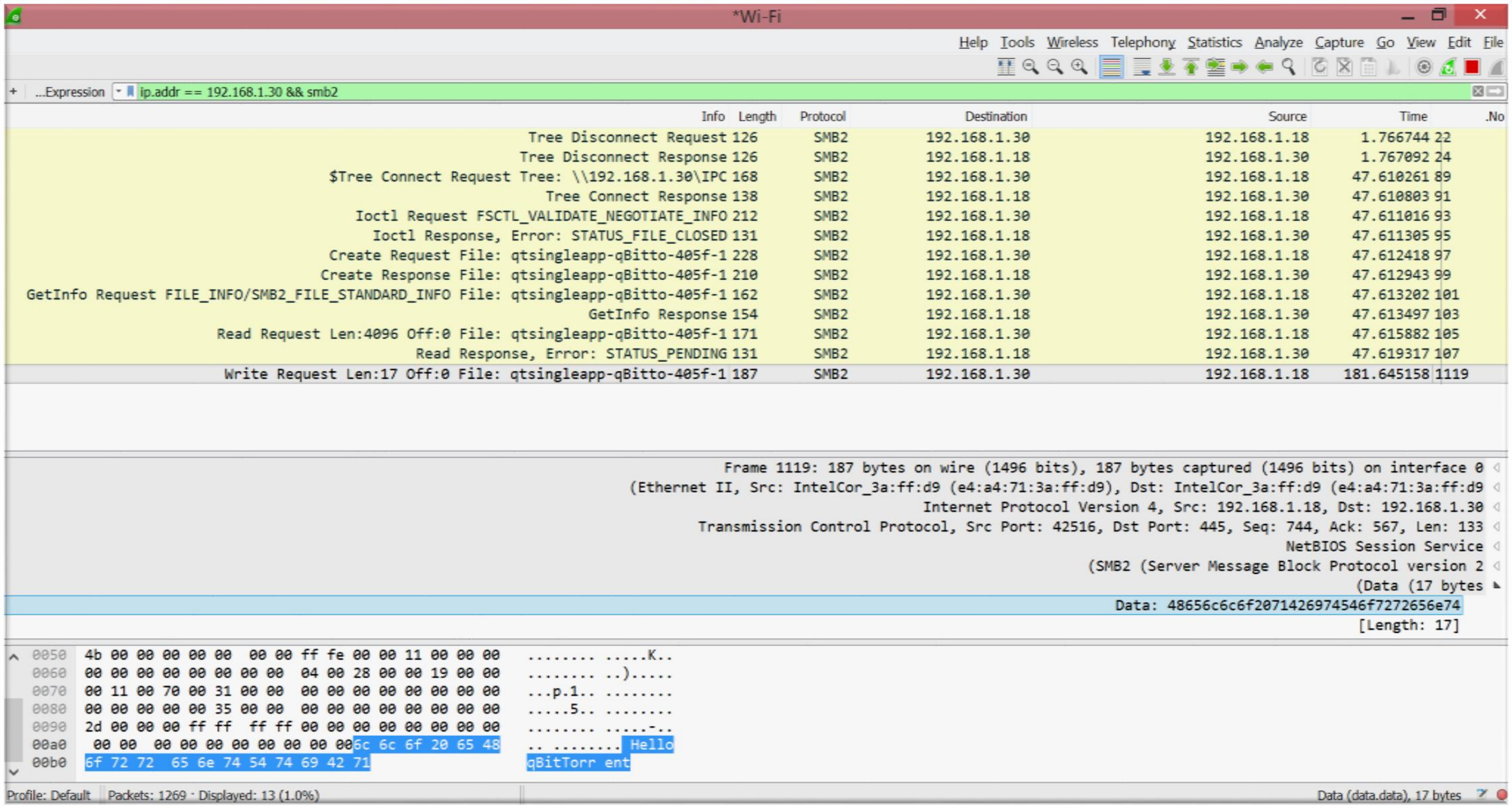
- Free for non-commercial usage ☺

NINJA CONVENTION

Sold Out!!!

Connecting To A Named Pipe

- This is how it looks in **Wireshark** (SMB communication)



*Wi-Fi
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
...Expression

```
ip.addr == 192.168.1.30 && smb2
```

```
                                                        Info Length  Protocol     Destination          Source        Time  .No
                                    Tree Disconnect Request 126      SMB2         192.168.1.30         192.168.1.18  1.766744 22
                                   Tree Disconnect Response 126      SMB2         192.168.1.18         192.168.1.30  1.767092 24
                  $Tree Connect Request Tree: \\192.168.1.30\IPC 168 SMB2         192.168.1.30         192.168.1.18  47.610261 89
                                     Tree Connect Response 138       SMB2         192.168.1.18         192.168.1.30  47.610803 91
                   Ioctl Request FSCTL_VALIDATE_NEGOTIATE_INFO 212   SMB2         192.168.1.30         192.168.1.18  47.611016 93
                     Ioctl Response, Error: STATUS_FILE_CLOSED 131   SMB2         192.168.1.18         192.168.1.30  47.611305 95
                 Create Request File: qtsingleapp-qBitto-405f-1 228  SMB2         192.168.1.30         192.168.1.18  47.612418 97
                Create Response File: qtsingleapp-qBitto-405f-1 210  SMB2         192.168.1.18         192.168.1.30  47.612943 99
GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: qtsingleapp-qBitto-405f-1 162 SMB2 192.168.1.30 192.168.1.18  47.613202 101
                                         GetInfo Response 154        SMB2         192.168.1.18         192.168.1.30  47.613497 103
      Read Request Len:4096 Off:0 File: qtsingleapp-qBitto-405f-1 171 SMB2        192.168.1.30         192.168.1.18  47.615882 105
                         Read Response, Error: STATUS_PENDING 131    SMB2         192.168.1.18         192.168.1.30  47.619317 107
        Write Request Len:17 Off:0 File: qtsingleapp-qBitto-405f-1 187 SMB2       192.168.1.30         192.168.1.18  181.645158 1119
```

```
              Frame 1119: 187 bytes on wire (1496 bits), 187 bytes captured (1496 bits) on interface 0
     (Ethernet II, Src: IntelCor_3a:ff:d9 (e4:a4:71:3a:ff:d9), Dst: IntelCor_3a:ff:d9 (e4:a4:71:3a:ff:d9
                                   Internet Protocol Version 4, Src: 192.168.1.18, Dst: 192.168.1.30
         Transmission Control Protocol, Src Port: 42516, Dst Port: 445, Seq: 744, Ack: 567, Len: 133
                                                                              NetBIOS Session Service
                                                      (SMB2 (Server Message Block Protocol version 2
                                                                                     (Data (17 bytes
                                                     Data: 48656c6c6f2071426974546f7272656e74
                                                                                       [Length: 17]
```

```
0050  4b 00 00 00 00 00  00 00 ff fe 00 00 11 00 00 00   ........ .....K..
0060  00 00 00 00 00 00 00 00  04 00 28 00 00 19 00 00   ........ ..).....
0070  00 11 00 70 00 31 00 00  00 00 00 00 00 00 00 00   ...p.1.. ........
0080  00 00 00 00 00 35 00 00  00 00 00 00 00 00 00 00   .....5.. ........
0090  2d 00 00 00 ff ff  ff ff 00 00 00 00 00 00 00 00   ........ .....-..
00a0   00 00  00 00 00 00 00 00 00 006c 6c 6f 20 65 48   .. ........ Hello
00b0  6f 72 72  65 6e 74 54 74 69 42 71                  qBitTorr ent
```

Profile: Default | Packets: 1269 · Displayed: 13 (1.0%) | Data (data.data), 17 bytes

Pipe ACLs And Connection Limitation

Pipe ACLs And Connection Limitation

- Named pipes are implemented by a filesystem driver in Windows NT, npfs.sys, which supports **security descriptors**

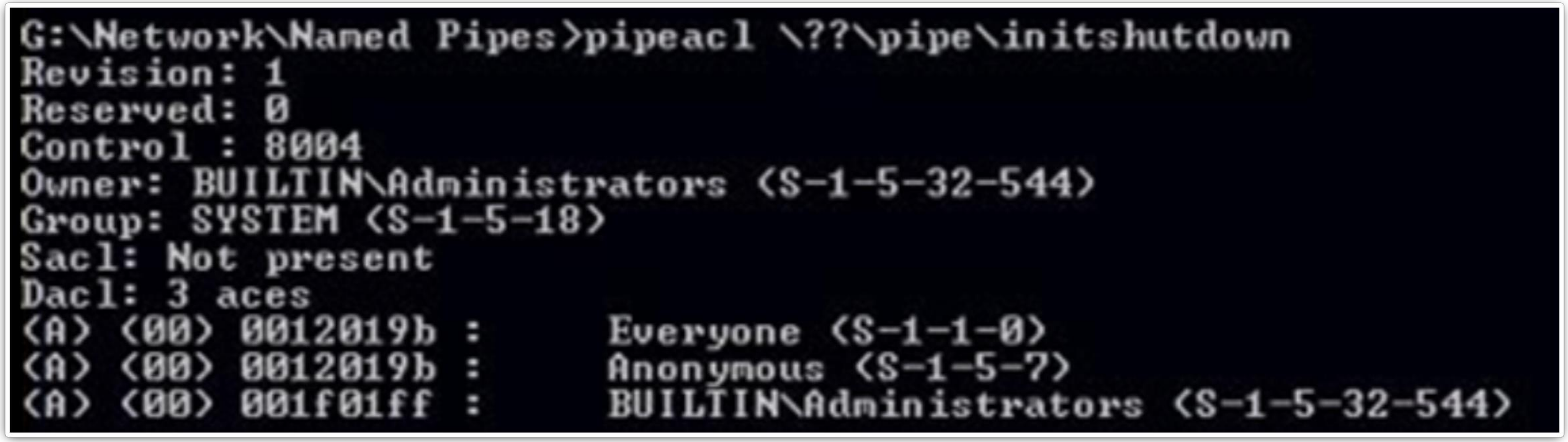
- Security descriptors are used to **control access** to named pipes.

- 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:

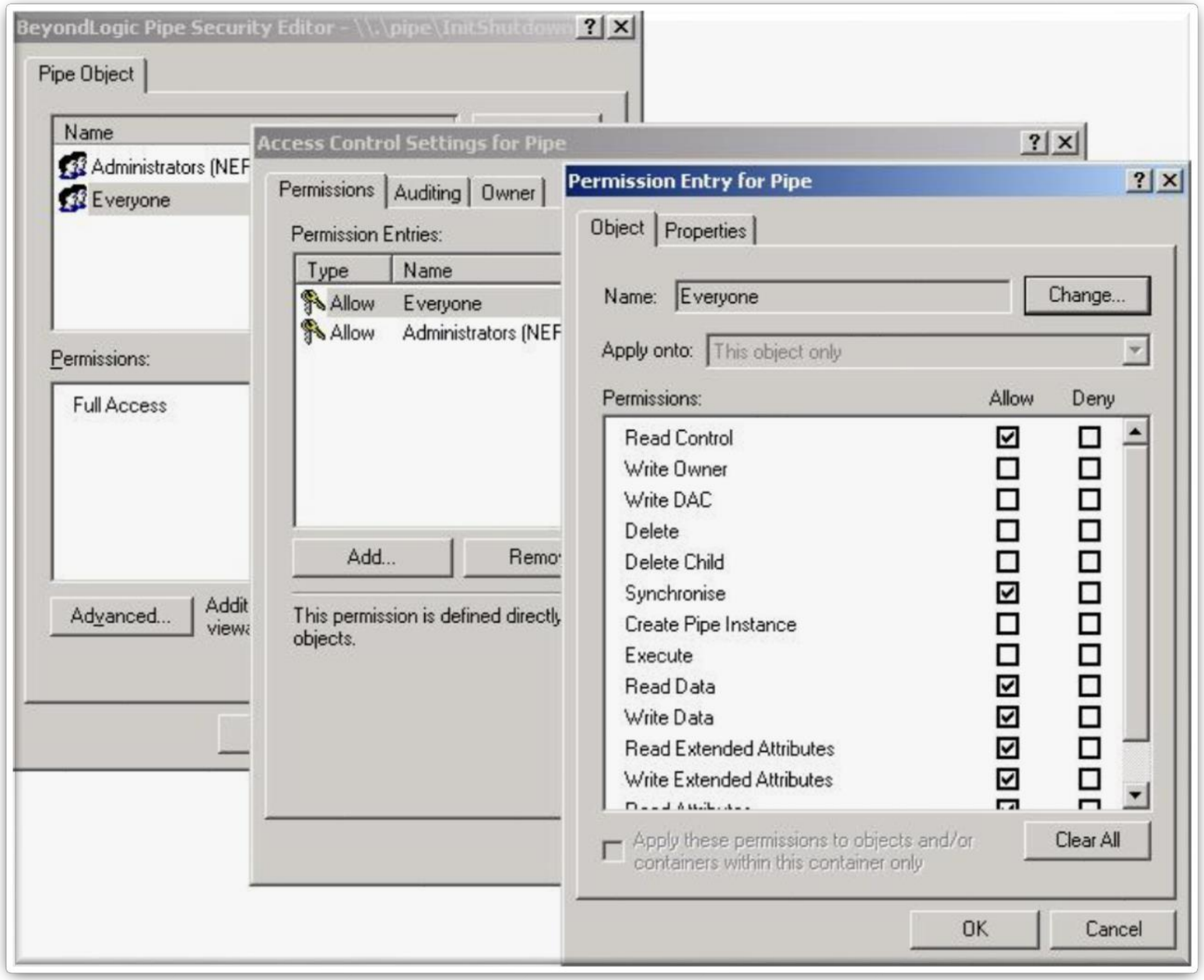


```
G:\Network\Named Pipes>pipeacl \??\pipe\initshutdown
Revision: 1
Reserved: 0
Control : 8004
Owner: BUILTIN\Administrators (S-1-5-32-544)
Group: SYSTEM (S-1-5-18)
Sacl: Not present
Dacl: 3 aces
(A) (00) 0012019b :      Everyone (S-1-1-0)
(A) (00) 0012019b :      Anonymous (S-1-5-7)
(A) (00) 001f01ff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



BeyondLogic Pipe Security Editor - \\.\pipe\InitShutdown

Pipe Object

Name

Administrators (NEF

Everyone

Permissions:

Full Access

Advanced... Addit view

Access Control Settings for Pipe

Permissions | Auditing | Owner

Permission Entries:

Type	Name
Allow	Everyone
Allow	Administrators (NEF

Add... Remo

This permission is defined directly objects.

Permission Entry for Pipe

Object | Properties

Name: Everyone Change...

Apply onto: This object only

Permissions:	Allow	Deny
Read Control	☑	□
Write Owner	□	□
Write DAC	□	□
Delete	□	□
Delete Child	□	□
Synchronise	☑	□
Create Pipe Instance	□	□
Execute	□	□
Read Data	☑	□
Write Data	☑	□
Read Extended Attributes	☑	□
Write Extended Attributes	☑	□
Read Attributes	☑	□

□ Apply these permissions to objects and/or containers within this container only

Clear All

OK Cancel

An old utility, deprecated

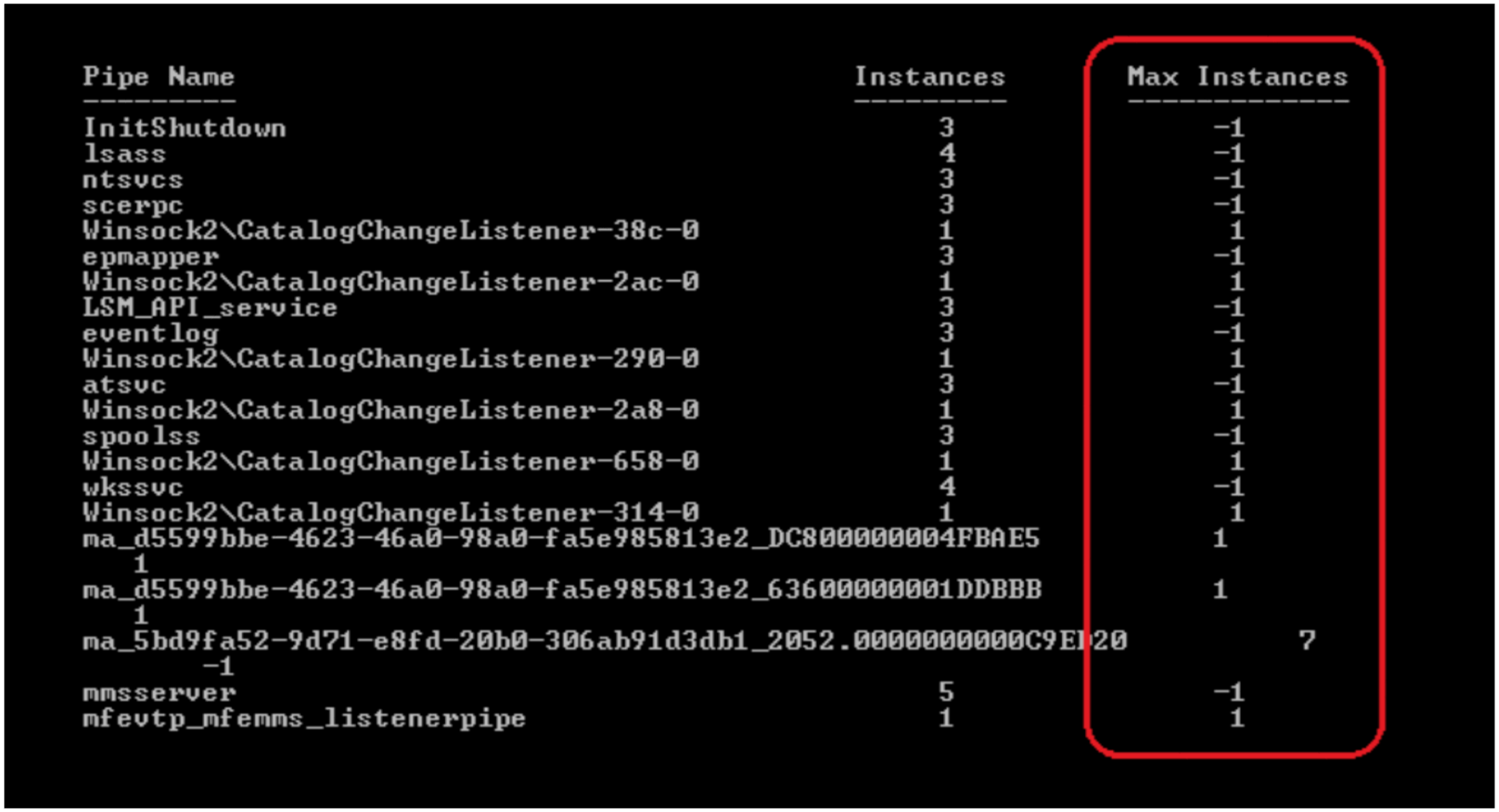
Win32 Pipe Security Editor
for Windows NT/2000/XP
http://retired.beyondlogic.org/solutions/pipesec/pipesec.htm

DEFCON

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_2052.0000000000C9ED20         7
       -1
mmsserver                                         5                -1
mfevtp_mfemms_listenerpipe                        1                 1
```

Named pipes in the wild

COMSEC Group
Cyber & Information Security

Conficker case study

- Conficker is a computer worm targeting the Microsoft Windows operating system that was first detected in November 2008.

- It uses flaws in Windows OS software and dictionary attacks on administrator passwords to propagate while forming a botnet.

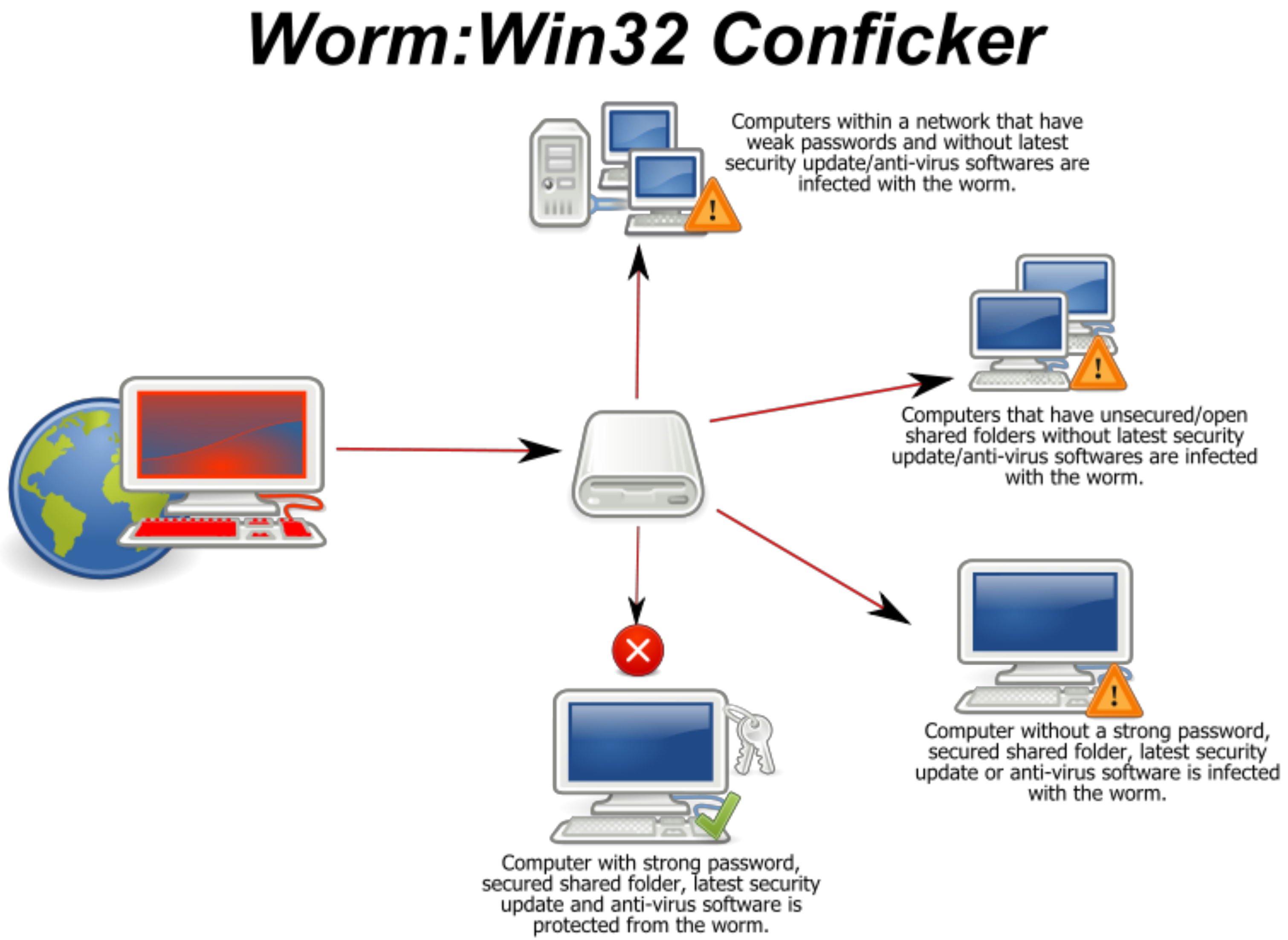
- It has been unusually difficult to counter because of its combined use of many advanced malware techniques.

- It infected millions of computers including government, business and home computers in over 190 countries (!).

DEFCON

COMSEC Group
Cyber & Information Security

Conficker case study



Computers within a network that have weak passwords and without latest security update/anti-virus softwares are infected with the worm.

Computers that have unsecured/open shared folders without latest security update/anti-virus softwares are infected with the worm.

Computer without a strong password, secured shared folder, latest security update or anti-virus software is infected with the worm.

Computer with strong password, secured shared folder, latest security update and anti-virus software is protected from the worm.

DEFCON

COMSEC Group
Cyber & Information Security

Conficker case study

- Variant C creates a **named pipe**, over which it can **push** URLs for downloadable payloads to other infected hosts on a local area network.

- Named pipes can be used for C&C purposes!

- Used in other Trojans as well: **Moker**, **ZxShell** and even **Petya** uses it to transfer extracted passwords.

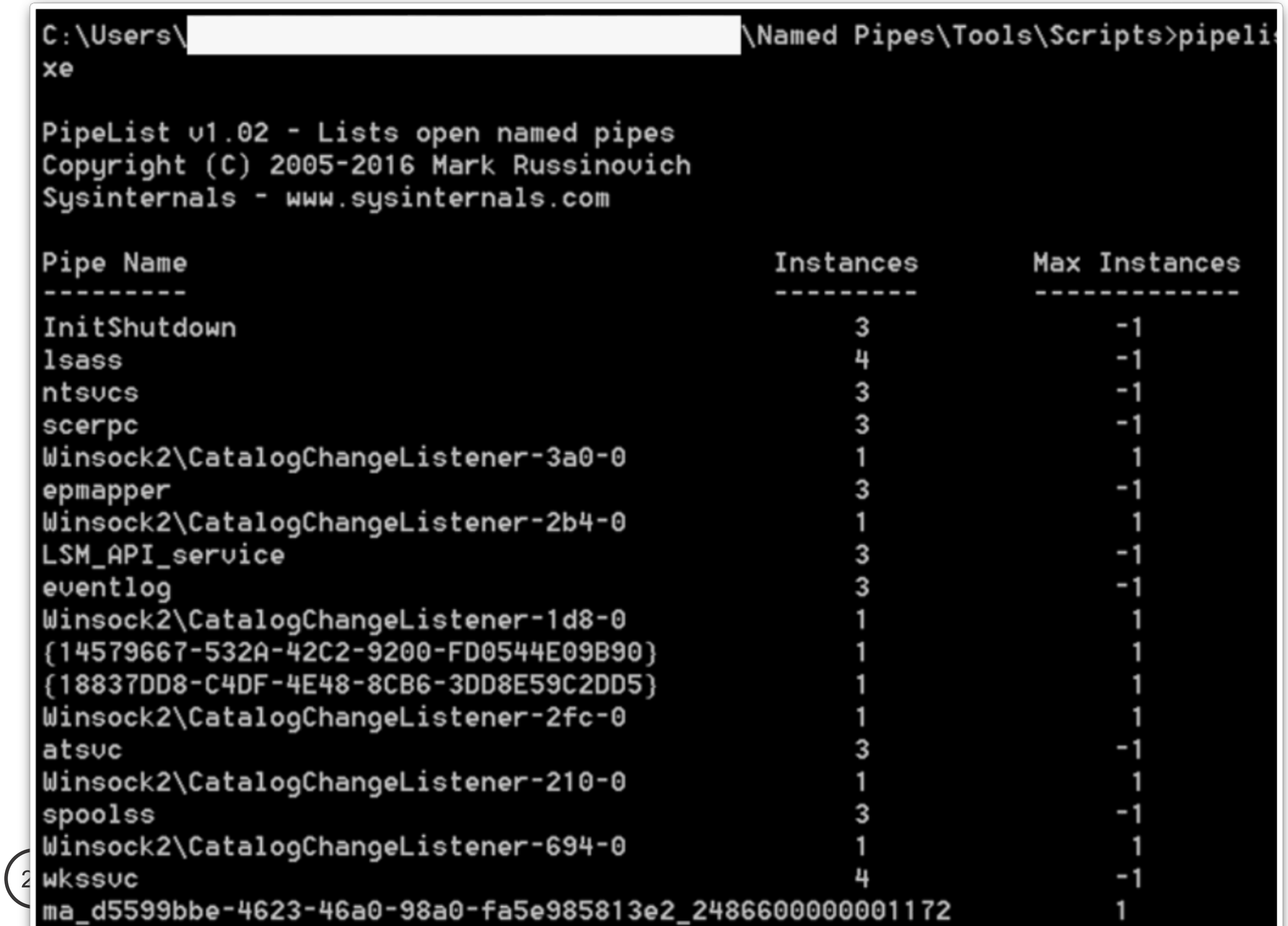
Enumerating And Scanning For Named Pipes

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\[redacted]\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

Enumerating And Scanning For Named Pipes

Named pipes ACLs enumeration

using SysInternals’ pipeacl

- enables viewing permission of a certain named pipes:

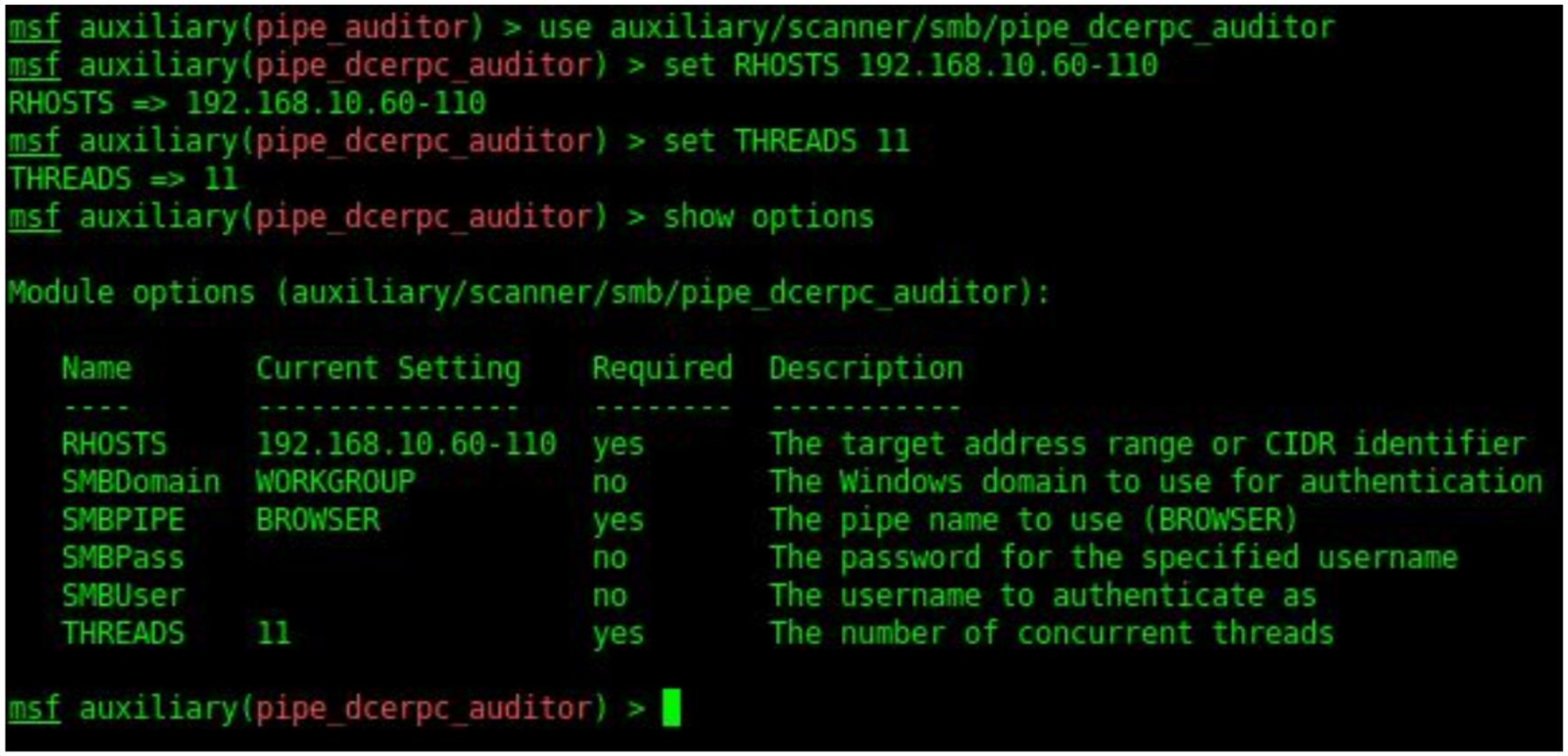
```
C:\> pipeacl \.\pipe\lsarpc

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

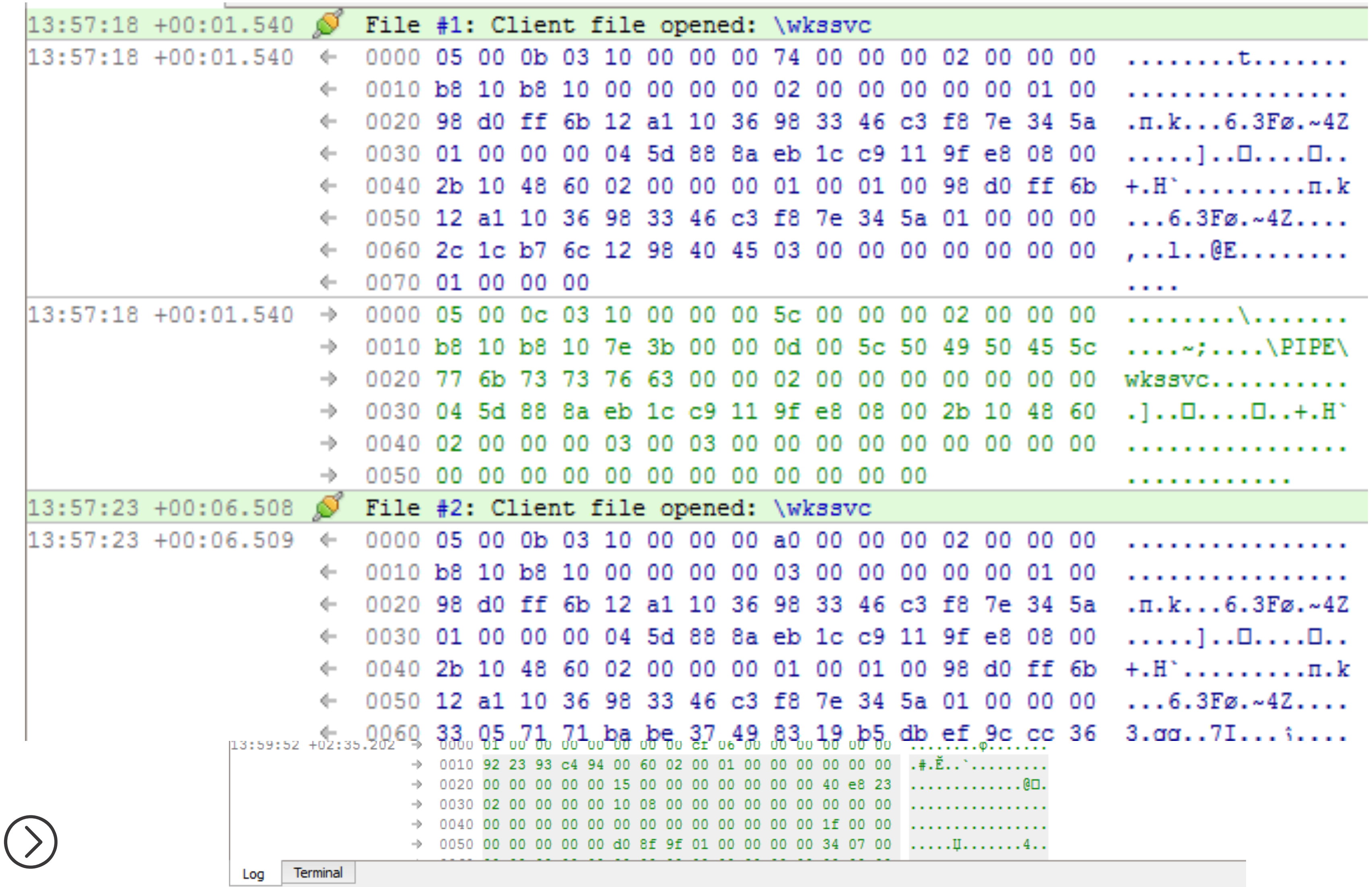
Sniffing Named Pipes Content

COMSEC Group
Cyber & Information Security

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              ............
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.σσ..7I...ì....
```

```
13:59:52 +02:35.202  →  0000 01 00 00 00 00 00 00 00 cf 06 00 00 00 00 00 00  ........φ.......
                     →  0010 92 23 93 c4 94 00 60 02 00 01 00 00 00 00 00 00  .#.Ĕ..`.........
                     →  0020 00 00 00 00 00 15 00 00 00 00 00 00 00 40 e8 23  .............@□.
                     →  0030 02 00 00 00 00 10 08 00 00 00 00 00 00 00 00 00  ................
                     →  0040 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 00  ................
                     →  0050 00 00 00 00 00 d0 8f 9f 01 00 00 00 00 34 07 00  .....Џ.......4..
```

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

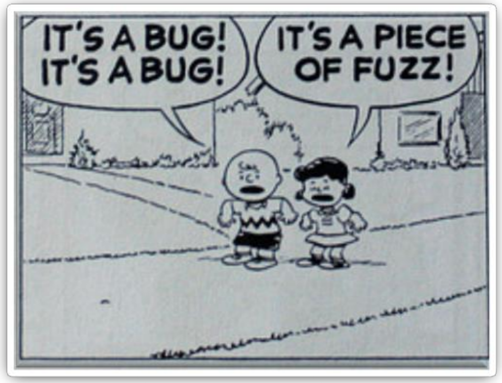
Two types of fuzzing approaches:

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

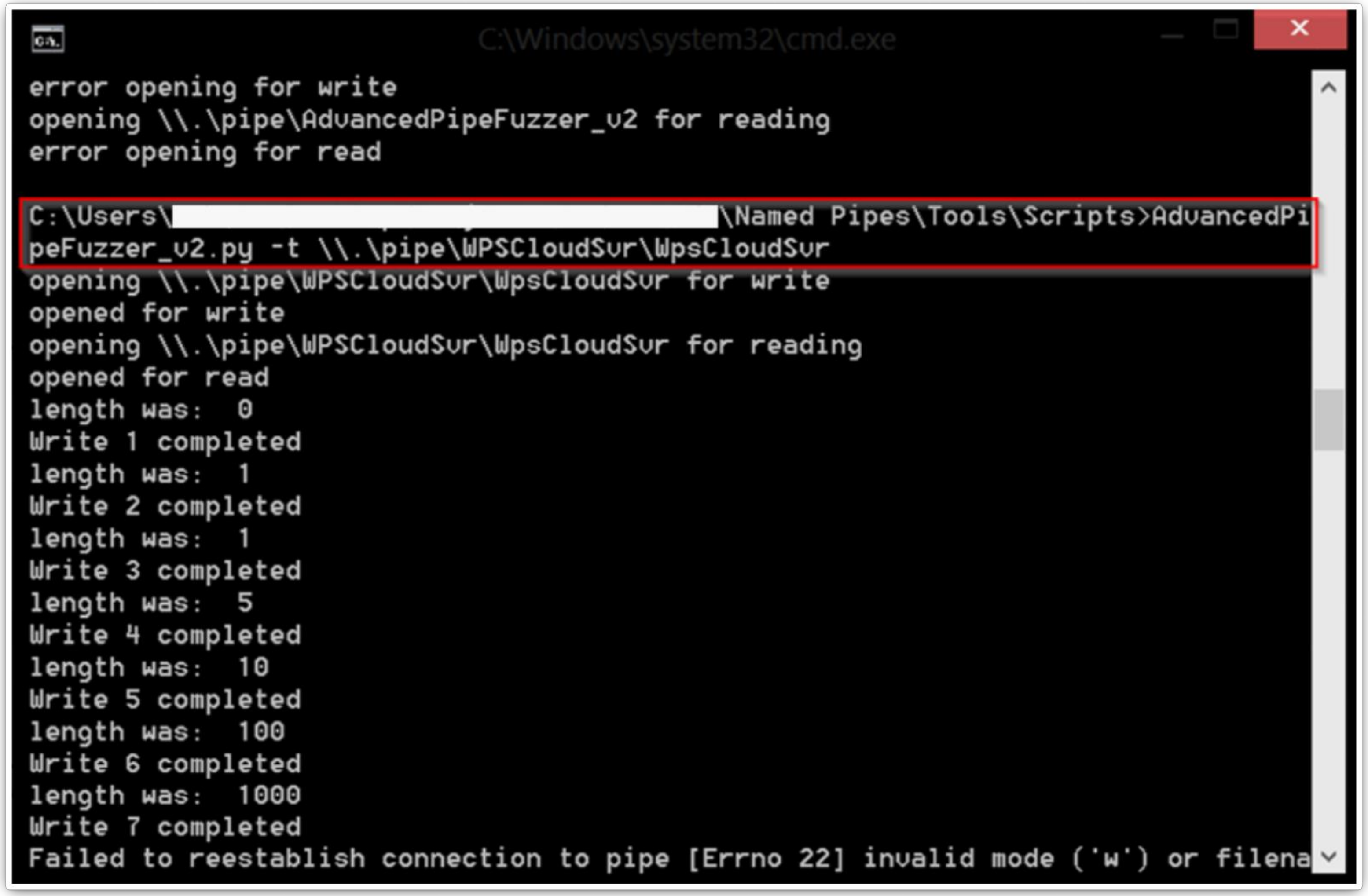
Smart ("White Box")

- 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



```
error opening for write
opening \\.\pipe\AdvancedPipeFuzzer_v2 for reading
error opening for read

C:\Users\[redacted]\Named Pipes\Tools\Scripts>AdvancedPi
peFuzzer_v2.py -t \\.\pipe\WPSCloudSvr\WpsCloudSvr
opening \\.\pipe\WPSCloudSvr\WpsCloudSvr for write
opened for write
opening \\.\pipe\WPSCloudSvr\WpsCloudSvr for reading
opened for read
length was:  0
Write 1 completed
length was:  1
Write 2 completed
length was:  1
Write 3 completed
length was:  5
Write 4 completed
length was:  10
Write 5 completed
length was:  100
Write 6 completed
length was:  1000
Write 7 completed
Failed to reestablish connection to pipe [Errno 22] invalid mode ('w') or filena
```

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

Exploitation And Impact

COMSEC Group
Cyber & Information Security

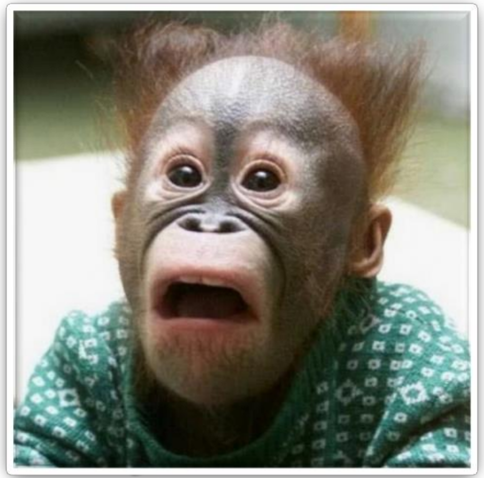
Exploitation And Impact

- 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**

- Named pipes fall **in between App PT and Infra PT**.
  - App pentesters usually connects to **typical app ports**, RPC and SMB **not included.**
  - When Infra pentesters encounter RPC\SMB they try to gain credentials, **not check for named pipes**.

- 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

Case study: Viber, qBittorrent, SugarSync

COMSEC Group
Cyber & Information Security

Viber, qBittorrent & SugarSync case study

Viber

- Cellular & endpoint social communication
- Free calls, text and picture sharing with anyone
- Competitors of WhatsApp
- 800 million users worldwide

Viber, 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

The applications use the widely used **QT framework**:

- A cross-platform application development framework for desktop, embedded and mobile. Supports multiple platforms and operating systems
- The 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** and in Qbitorrent, also a possible **remote command injection**

Demo

Mitigation And Defense

COMSEC Group
Cyber & Information Security

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

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! ☺

DEFCON

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

DEFCON

COMSEC Group
Cyber & Information Security