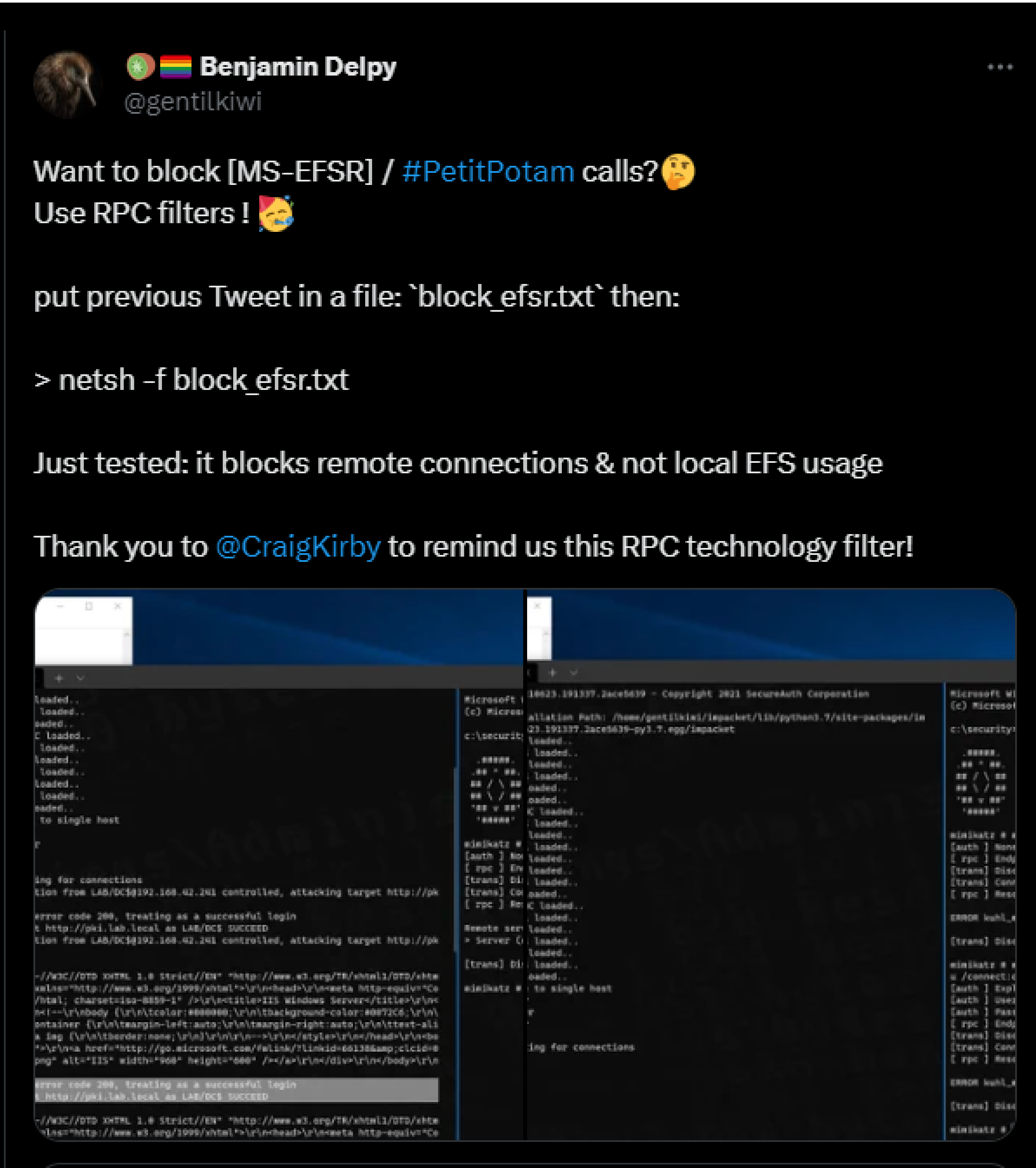
:(

RPC Filter? I Hardly Know Her!

BSides Philly 2023

slides
https://github.com/SecurityRiskAdvisors/public-assets

BSides Philly – RPC Filter? I Hardly Know Her!



Benjamin Delpy
@gentilkiwi

Want to block [MS-EFSR] / #PetitPotam calls?🤔
Use RPC filters ! 🥳

put previous Tweet in a file: `block_efsr.txt` then:

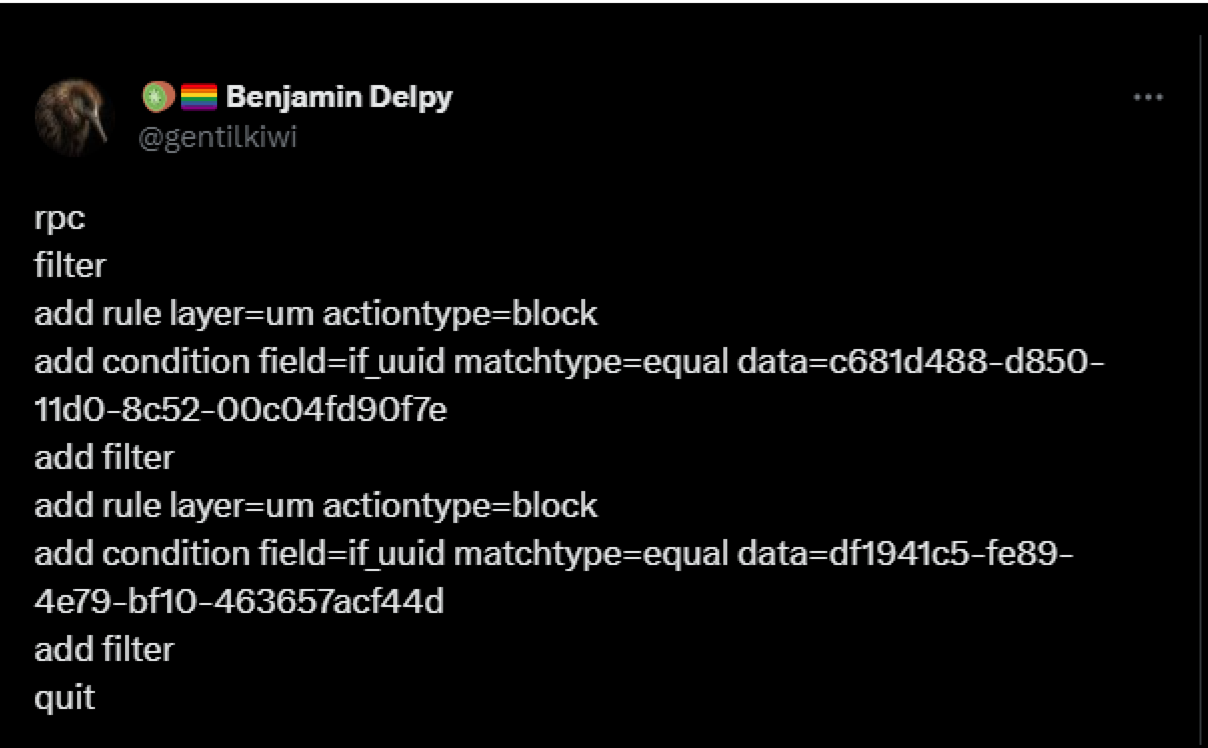
> netsh -f block_efsr.txt

Just tested: it blocks remote connections & not local EFS usage

Thank you to @CraigKirby to remind us this RPC technology filter!

```
loaded..
 loaded..
oaded..
C loaded..
 loaded..
loaded..
 loaded..
loaded..
 loaded..
oaded..
 to single host

r

ing for connections
tion from LAB/DC$@192.168.42.241 controlled, attacking target http://pk

error code 200, treating as a successful login
t http://pki.lab.local as LAB/DC$ SUCCEED
tion from LAB/DC$@192.168.42.241 controlled, attacking target http://pk

-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtm
xmlns="http://www.w3.org/1999/xhtml">\r\n<head>\r\n<meta http-equiv="Co
/html; charset=iso-8859-1" />\r\n<title>IIS Windows Server</title>\r\n<
n<!--\r\nbody {\r\n\tcolor:#000000;\r\n\tbackground-color:#0072C6;\r\n\
ontainer {\r\n\tmargin-left:auto;\r\n\tmargin-right:auto;\r\n\ttext-ali
a img {\r\n\tborder:none;\r\n}\r\n\r\n-->\r\n</style>\r\n</head>\r\n<bo
">\r\n<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0
png" alt="IIS" width="960" height="600" /></a>\r\n</div>\r\n</body>\r\n

error code 200, treating as a successful login
t http://pki.lab.local as LAB/DC$ SUCCEED

-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtm
xmlns="http://www.w3.org/1999/xhtml">\r\n<head>\r\n<meta http-equiv="Co
```

```
10623.191337.2ace5639 - Copyright 2021 SecureAuth Corporation

allation Path: /home/gentilkiwi/impacket/lib/python3.7/site-packages/im
23.191337.2ace5639-py3.7.egg/impacket
loaded..
 loaded..
loaded..
 loaded..
oaded..
oaded..
C loaded..
 loaded..
loaded..
 loaded..
loaded..
loaded..
 loaded..
oaded..
C loaded..
 loaded..
loaded..
 loaded..
loaded..
 loaded..
oaded..
 to single host

r

ing for connections
```



Benjamin Delpy
@gentilkiwi

```
rpc
filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=c681d488-d850-11d0-8c52-00c04fd90f7e
add filter
add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=df1941c5-fe89-4e79-bf10-463657acf44d
add filter
quit
```

```
C:\Users\Evan Perotti> whoami

Work                                  Links
----                                  -----

Employer Role                         Site Handle
======== ===============              ==== ================
SRA      Lead Scientist               𝕏    @2xxeformyshirt
```

BSides Philly 2023

- Background
- RPC Filters
- Defense
- Implementation
- Limitations
- Closing

```
#> cls
#> echo %SECTION%
```

BACKGROUND

#> RPC: **Remote Procedure Call**

#> Client-server mechanism for IPC

#> Local (same system) and remote

#> Remote; commonly via TCP and SMB named pipes

#> Interfaces and procedures

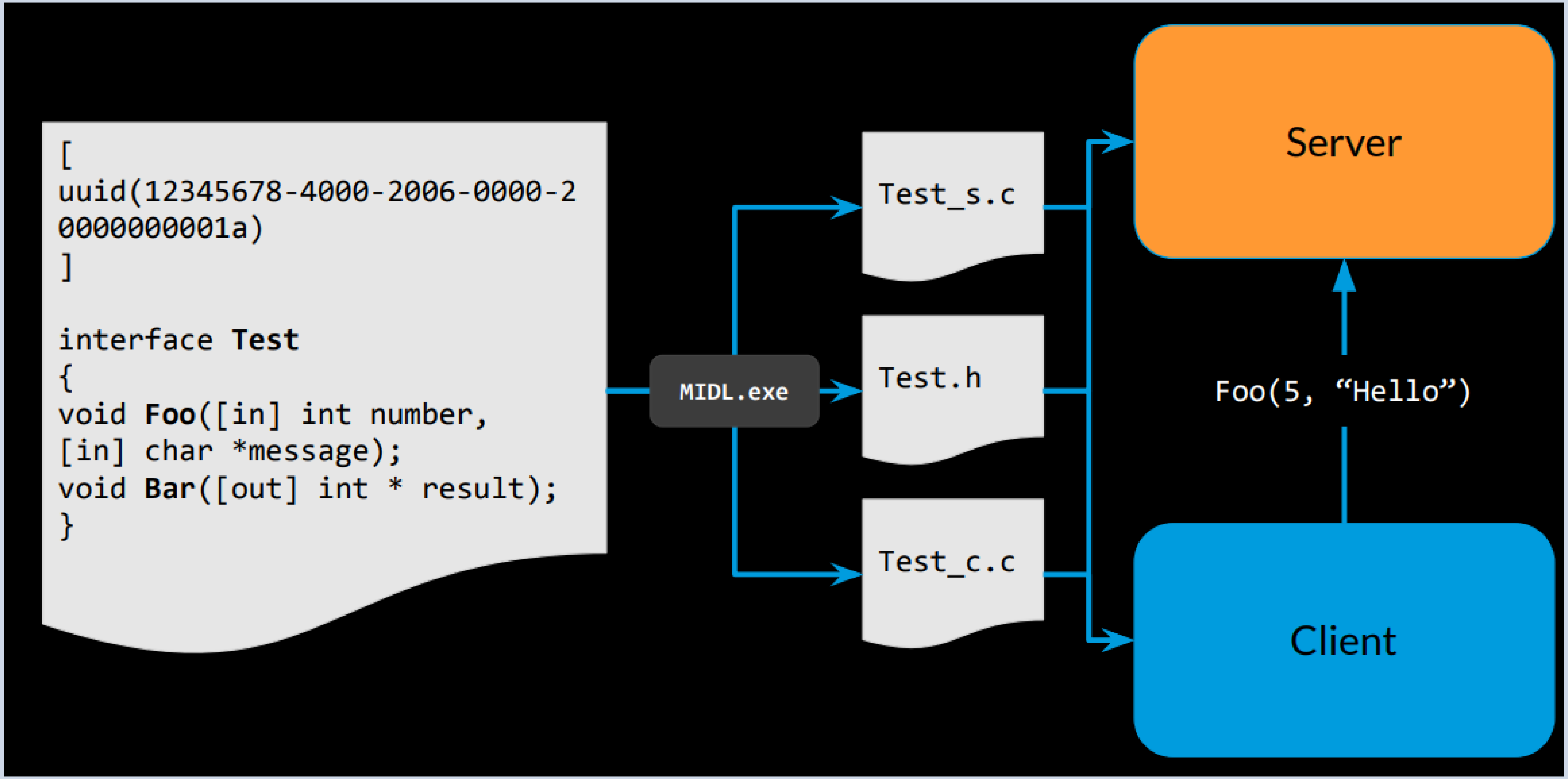
#> Procedures =
individual methods

#> Interfaces =
overarching groups of related methods

```
#> Service Control Manager example

#> Create a Windows service
   = RCreateServiceW
   = opnum 12

#> Create service + delete service + …
   = interface



#> note: will continue to user service creation for example
```

BSides Philly – RPC Filter? I Hardly Know Her!

File Home View



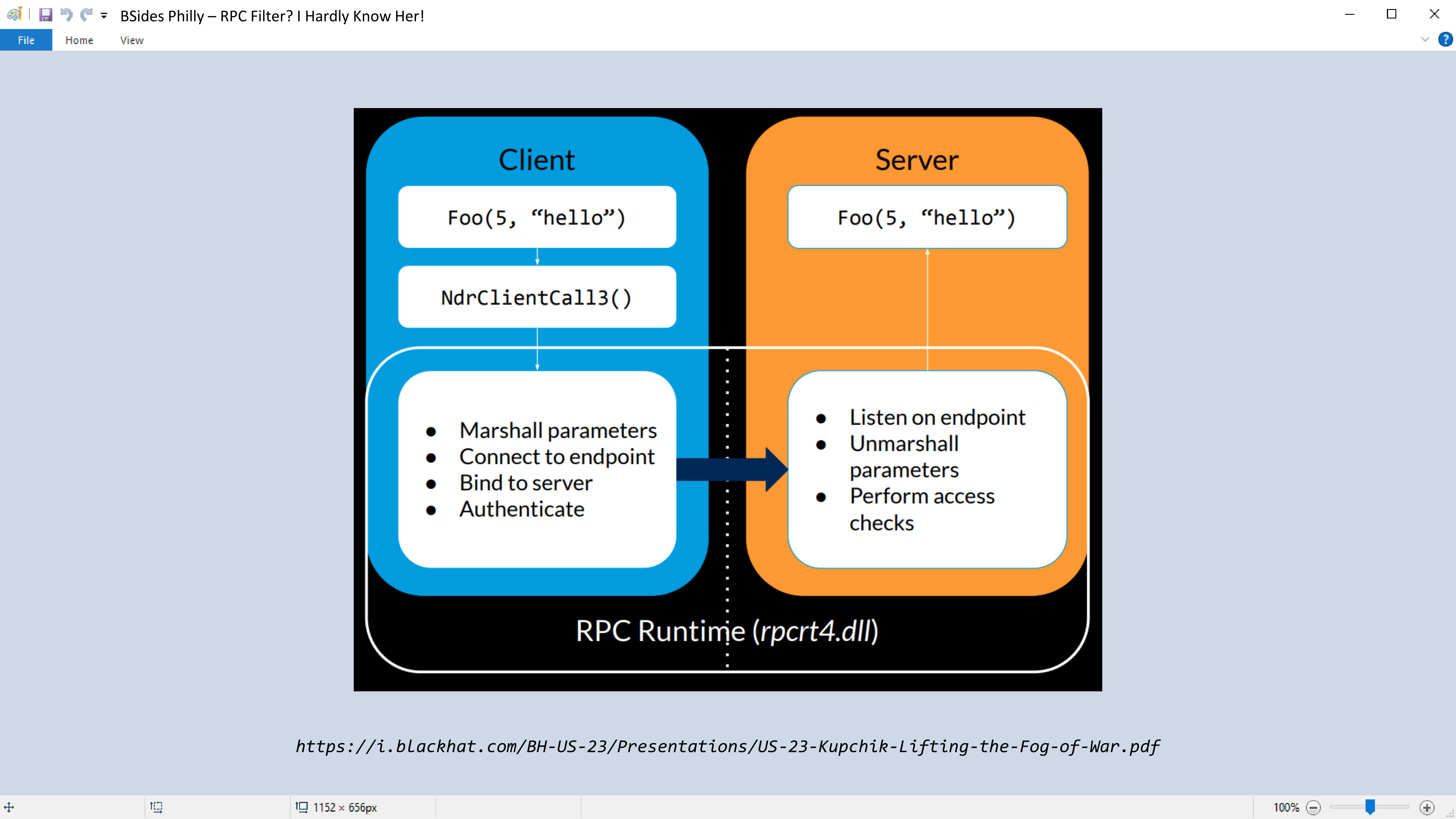
```
[
uuid(12345678-4000-2006-0000-2
0000000001a)
]

interface Test
{
void Foo([in] int number,
[in] char *message);
void Bar([out] int * result);
}
```

https://i.blackhat.com/BH-US-23/Presentations/US-23-Kupchik-Lifting-the-Fog-of-War.pdf

1152 × 656px

100%

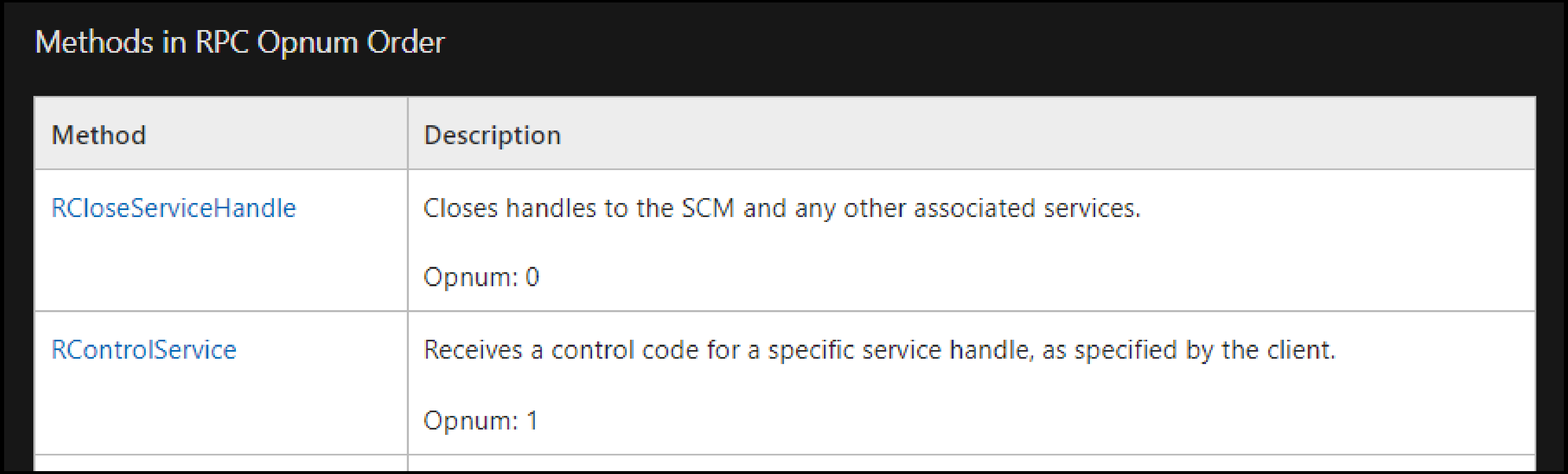
BSides Philly – RPC Filter? I Hardly Know Her!



https://i.blackhat.com/BH-US-23/Presentations/US-23-Kupchik-Lifting-the-Fog-of-War.pdf

#> RPC is often documented

#> Example: Service Control Manager



Methods in RPC Opnum Order

Method	Description
RCloseServiceHandle	Closes handles to the SCM and any other associated services. Opnum: 0
RControlService	Receives a control code for a specific service handle, as specified by the client. Opnum: 1

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-scmr/0d7a7011-9f41-470d-ad52-8535b47ac282

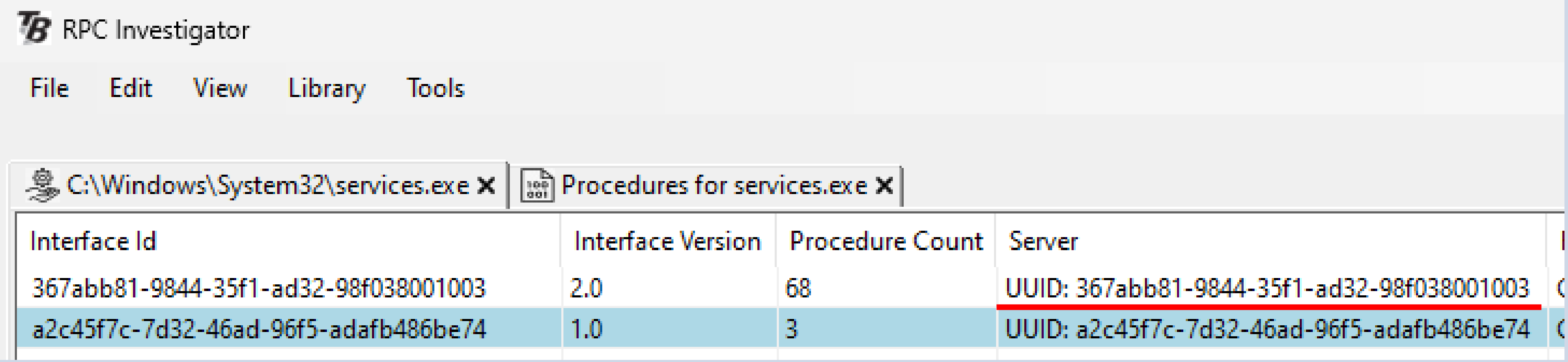
#> RPC Investigator by Trail of Bits

#> Can be used to find interface/procedures

#> https://github.com/trailofbits/RpcInvestigator

#> Especially useful for undocumented interfaces

Load service.exe



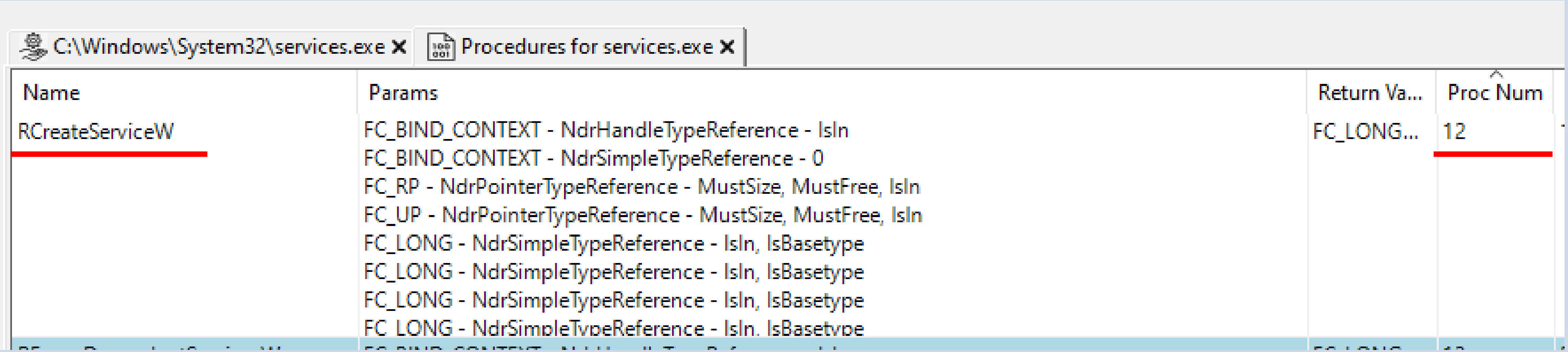
Interface Id	Interface Version	Procedure Count	Server
367abb81-9844-35f1-ad32-98f038001003	2.0	68	UUID: 367abb81-9844-35f1-ad32-98f038001003
a2c45f7c-7d32-46ad-96f5-adafb486be74	1.0	3	UUID: a2c45f7c-7d32-46ad-96f5-adafb486be74

notice the 367… interface ID

BSides Philly – RPC Filter? I Hardly Know Her!

File Home View

Load procedure for interface



Name	Params	Return Va...	Proc Num
RCreateServiceW	FC_BIND_CONTEXT - NdrHandleTypeReference - IsIn FC_BIND_CONTEXT - NdrSimpleTypeReference - 0 FC_RP - NdrPointerTypeReference - MustSize, MustFree, IsIn FC_UP - NdrPointerTypeReference - MustSize, MustFree, IsIn FC_LONG - NdrSimpleTypeReference - IsIn, IsBasetype FC_LONG - NdrSimpleTypeReference - IsIn, IsBasetype FC_LONG - NdrSimpleTypeReference - IsIn, IsBasetype FC_LONG - NdrSimpleTypeReference - IsIn, IsBasetype	FC_LONG...	12

notice the proc num (opnum) of 12

1152 × 656px

100%

```
#> cls
#> echo %SECTION%
```

ATTACKS

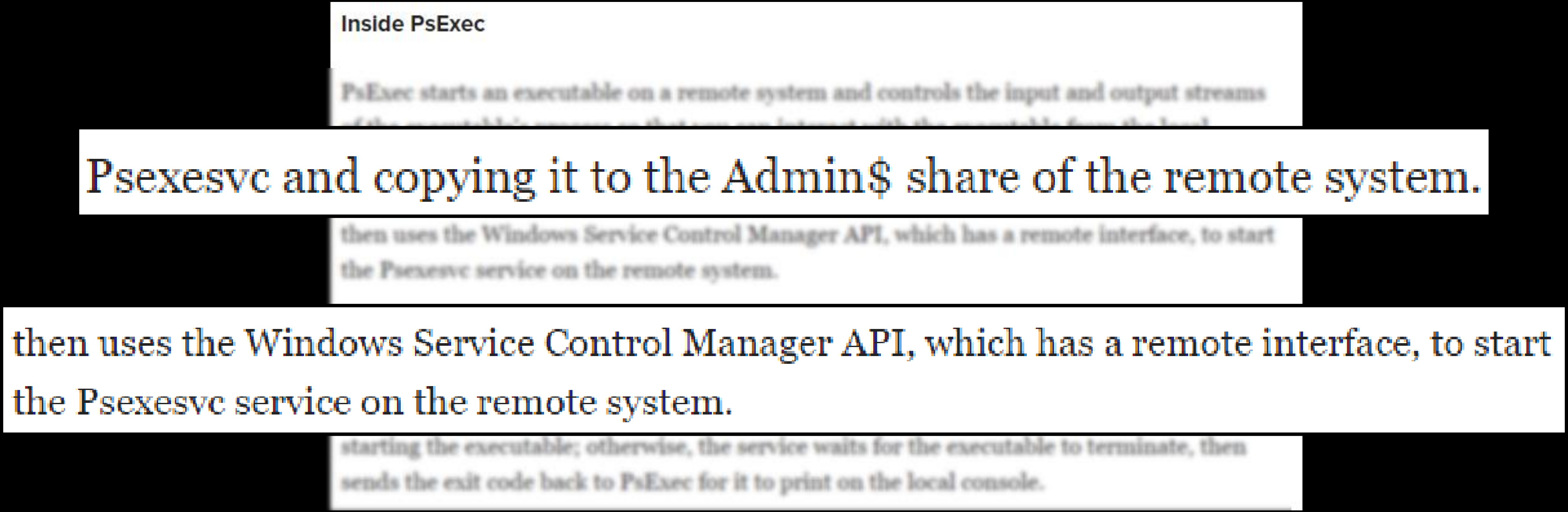
```
#> Underpins many common attacks, including

     > DCSync
     > PsExec
     > PetitPotam
     > Printer Bug
     > Zerologon
     > …
```

https://github.com/jsecurity101/MSRPC-to-ATTACK

RPC Interface	Interface ID	Example Attack
Distributed File System Namespace Management	4FC742E0-4A10-11CF-8273-00AA004AE673	DFSCoerce – coercion attack
Directory Replication Service	e3514235-4b06-11d1-ab04-00c04fc2dcd2	DCSync – password hash retrieval
Encrypting File System	c681d488-d850-11d0-8c52-00c04fd90f7e df1941c5-fe89-4e79-bf10-463657acf44d	PetitPotam – coercion attack
File Server Remote VSS	a8e0653c-2744-4389-a61d-7373df8b2292	ShadowCoerce – coercion attack
LSA Remote	12345778-1234-ABCD-EF00-0123456789AB	Enumeration
Netlogon	12345678-1234-ABCD-EF00-01234567CFFB	Zerologon
Print System Remote	12345678-1234-ABCD-EF00-0123456789AB 76F03F96-CDFD-44FC-A22C-64950A001209	Printer Bug – coercion attack Print Nightmare – RCE
Registry Remote	338CD001-2244-31F1-AAAA-900038001003	Persistence, etc
SAM Remote	12345778-1234-ABCD-EF00-0123456789AC	Net commands
Service Control Manager	367ABB81-9844-35F1-AD32-98F038001003	PsExec
Server Service Remote	4b324fc8-1670-01d3-1278-5a47bf6ee188	Bloodhound Session collection
Tasks Scheduler	1FF70682-0A51-30E8-076D-740BE8CEE98 378E52B0-C0A9-11CF-822D-00AA0051E40F 86D35949-83C9-4044-B424-DB363231FD0C	Scheduled task lateral movement
Workstation Service	6BFFD098-A112-3610-9833-46C3F87E345A	Bloodhound logged on users

#> PsExec

```
CMD> psexec -i \\target cmd
```



Inside PsExec

PsExec starts an executable on a remote system and controls the input and output streams of the executable's process so that you can interact with the executable from the local

Psexesvc and copying it to the Admin$ share of the remote system.

then uses the Windows Service Control Manager API, which has a remote interface, to start the Psexesvc service on the remote system.

then uses the Windows Service Control Manager API, which has a remote interface, to start the Psexesvc service on the remote system.

starting the executable; otherwise, the service waits for the executable to terminate, then sends the exit code back to PsExec for it to print on the local console.

https://www.itprotoday.com/windows-server/psexec-explainer-mark-russinovich

BSides Philly – RPC Filter? I Hardly Know Her!

File Home View

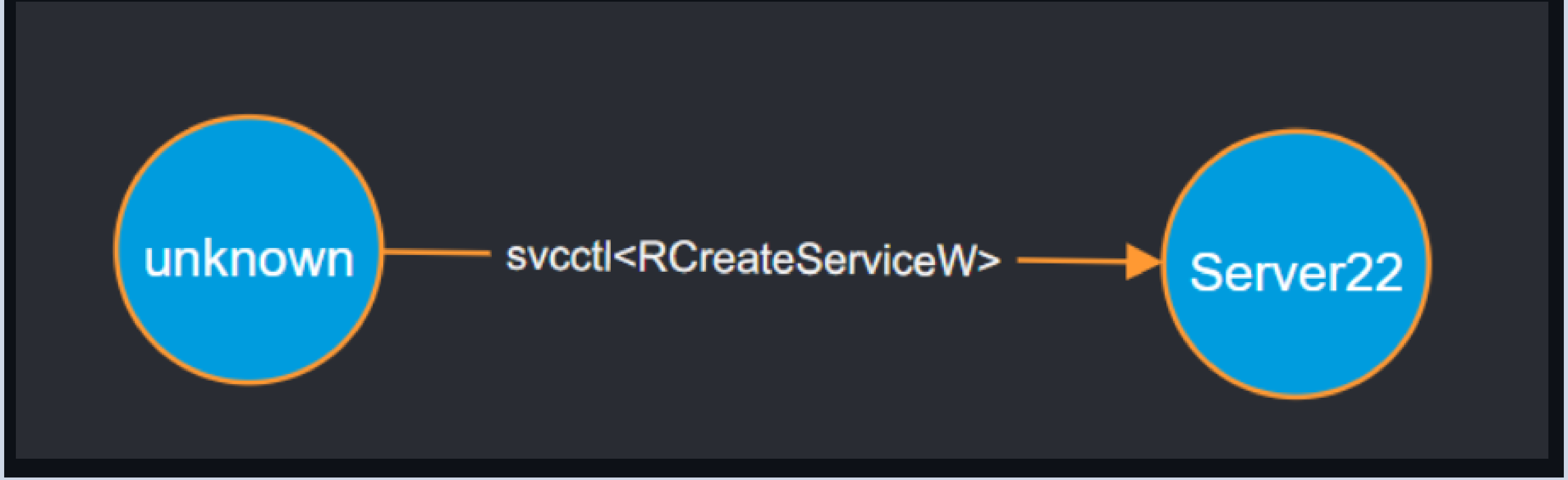
RCreateServiceW

Creates a service and adds it to the specified SCM database.

Opnum: 12

PSExec

```
Match p=(s:Computer)-[r:Connects]->(d:Computer)
Where s.hostname <> d.hostname
AND r.interface_uuid = "367abb81-9844-35f1-ad32-98f038001003" AND r.opnum = 12
Return p
```



https://github.com/akamai/akamai-security-research/tree/main/rpc_toolkit/rpc_visibility

1152 × 656px 100%

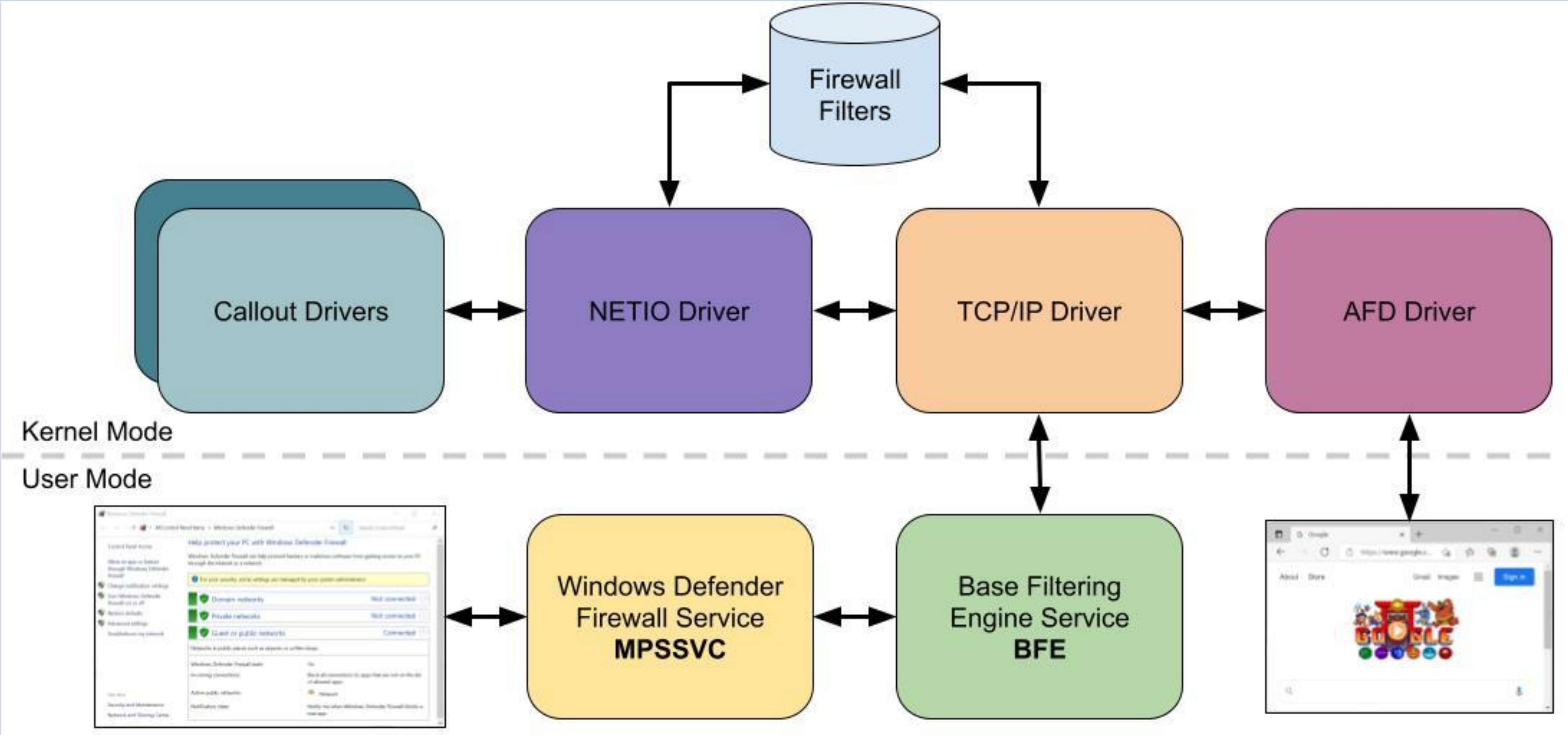
```
#> cls
#> echo %SECTION%
```

FILTERS

```
#> Windows Filtering Platform (WFP)

     > OS-level network connection blocking
     > supports firewall-like and similar
       application
     > Windows Firewall uses WFP


#> Base Filtering Engine

     > Manages the filter rules for WFP
```

BSides Philly – RPC Filter? I Hardly Know Her!

File Home View

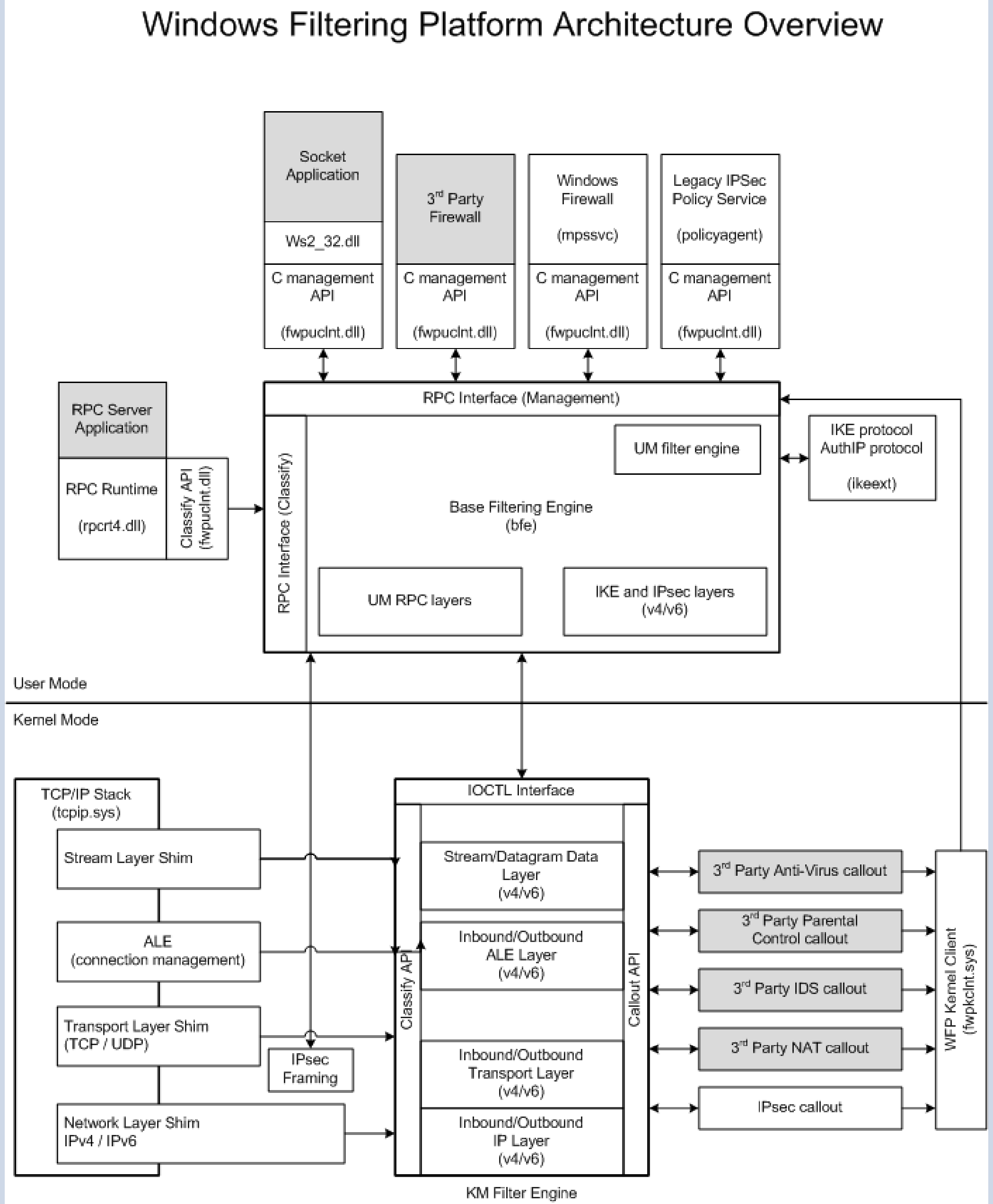


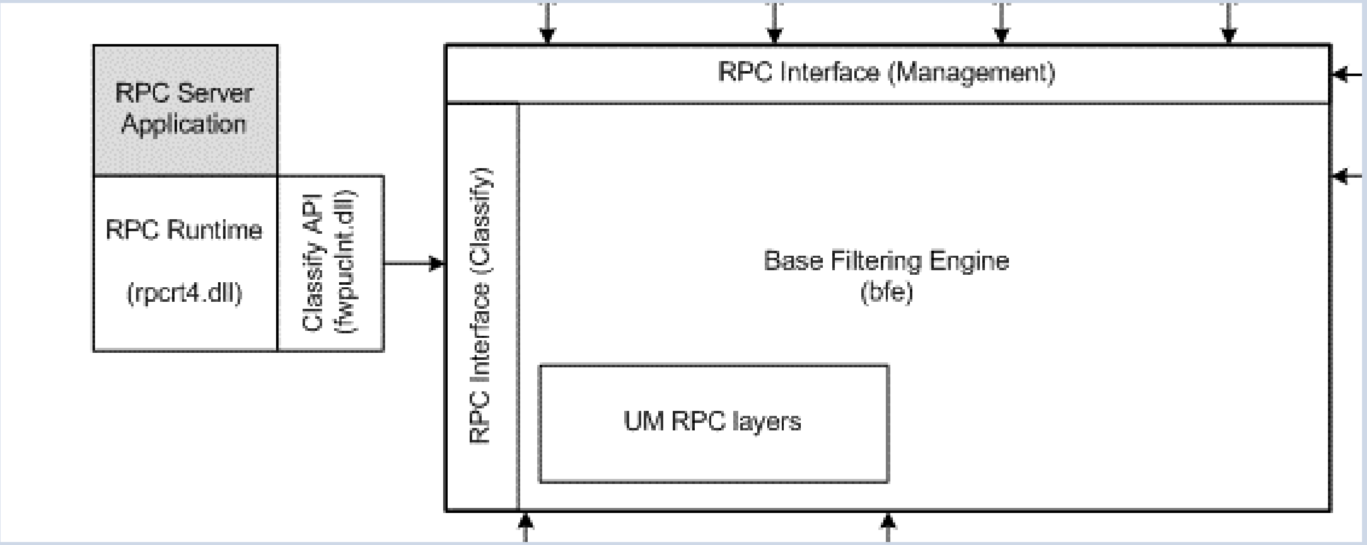
https://googleprojectzero.blogspot.com/2021/08/understanding-network-access-windows-app.html

1152 × 656px 100%

BSides Philly – RPC Filter? I Hardly Know Her!

File Home View





https://learn.microsoft.com/en-us/windows/win32/fwp/windows-filtering-platform-architecture-overview

1152 × 656px 100%

#> RPC Filters

#> Block/audit/allow RPC connections

#> Multiple filtering characteristics

#> All-or-nothing for interfaces

#> More details see: https://www.tiraniddo.dev/2021/08/how-windows-firewall-rpc-filter-works.html

#> Notable filtering fields

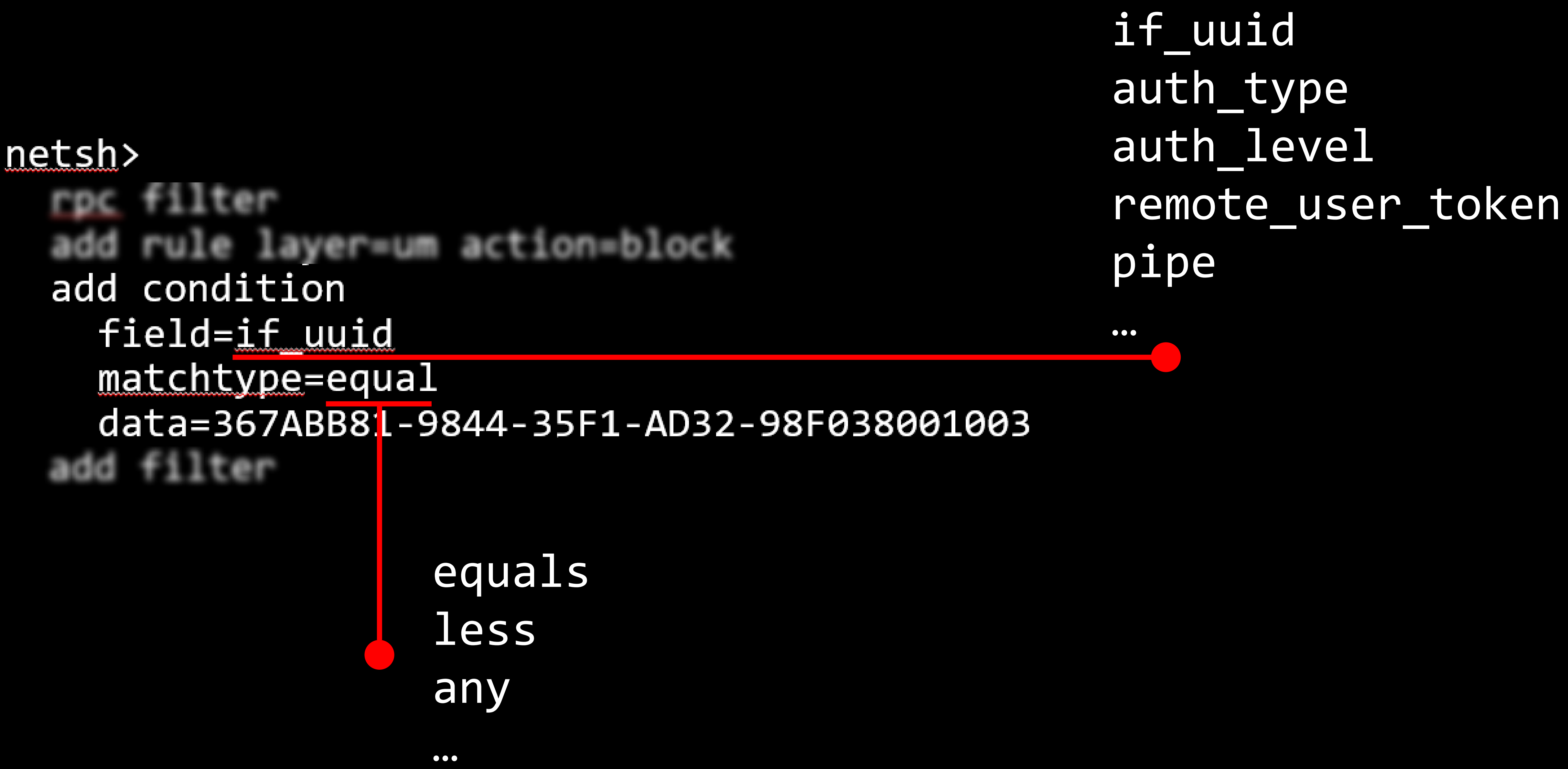
> Interface UUID and version
> Protocol (e.g. named pipes, TCP)
> Auth info (e.g. Kerberos, NTLM)
> User token
> ~~Pipe name~~

```
#> Example rule creation

     netsh>
       rpc filter
       add rule layer=um action=block
       add condition
         field=if_uuid
         matchtype=equal
         data=367ABB81-9844-35F1-AD32-98F038001003
       add filter
```

```
netsh>
  rpc filter
  add rule layer=um action=block
  add condition
    field=if_uuid
    matchtype=equal
    data=367ABB81-9844-35F1-AD32-98F03800100
  add filter
```

um
epmap
ep_add
proxy_conn
proxy_if

block
permit
audit



```
netsh>
  rpc filter
  add rule layer=um action=block
  add condition
    field=if_uuid
    matchtype=equal
    data=367ABB81-9844-35F1-AD32-98F038001003
  add filter
```

```
if_uuid
auth_type
auth_level
remote_user_token
pipe
…
```

```
equals
less
any
…
```

```
#> Example conditions

netsh> add condition
          field=if_uuid matchtype=equal
          data=367ABB81-9844-35F1-AD32-98F038001003



translated: interface == Service Control Manager
```

#> Example conditions (cont’d)

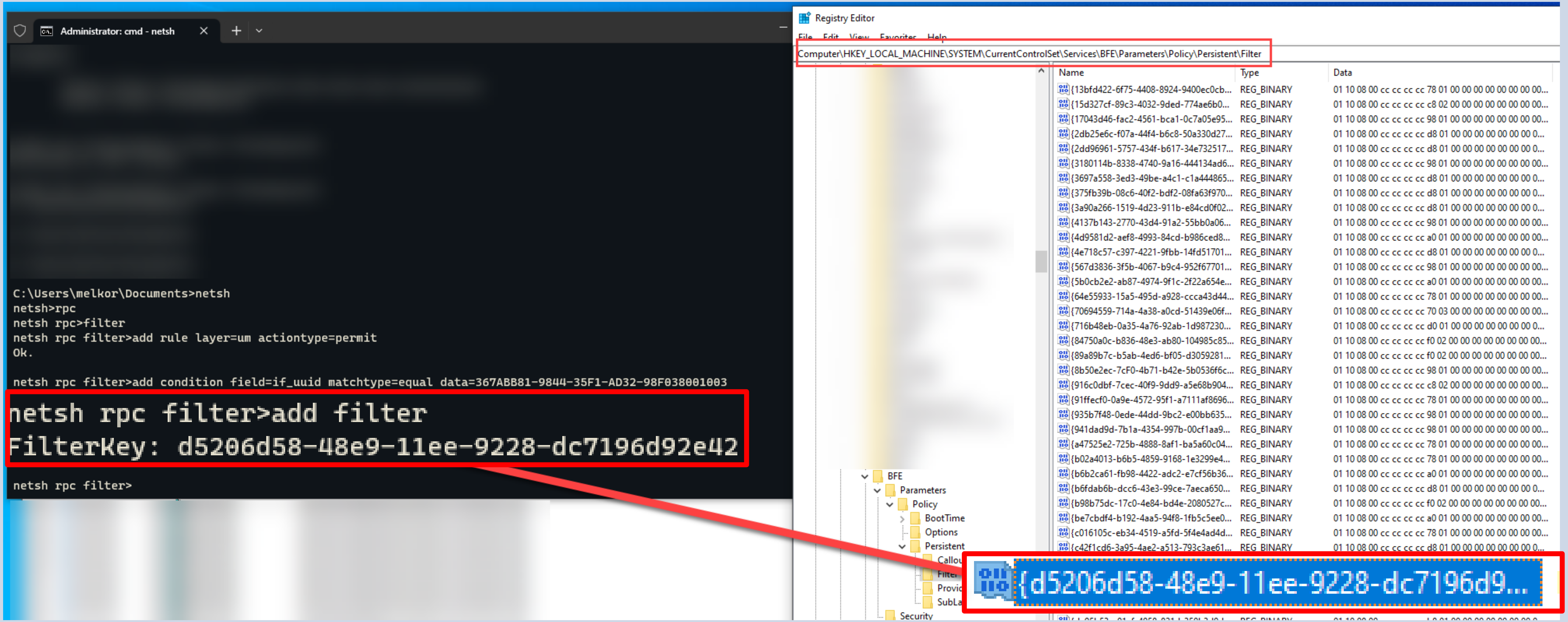
```
netsh> add condition
         field=auth_type matchtype=equal
         data=16
```

```
translated: Auth == Kerberos
```

#> Example conditions (cont’d)

```
netsh> add condition
        field=remote_user_token matchtype=equal
        data=D:(A;;CC;;;S-1-5-21-3564508084-
                    3432644214-2145392011-1122)


translated: User’s Group == domain\group
```

BSides Philly – RPC Filter? I Hardly Know Her!



```
[redacted]

C:\Users\melkor\Documents>netsh
netsh>rpc
netsh rpc>filter
netsh rpc filter>add rule layer=um actiontype=permit
Ok.

netsh rpc filter>add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32-98F038001003
netsh rpc filter>add filter
FilterKey: d5206d58-48e9-11ee-9228-dc7196d92e42

netsh rpc filter>
```

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BFE\Parameters\Policy\Persistent\Filter

Name	Type	Data
{13bfd422-6f75-4408-8924-9400ec0cb...	REG_BINARY	01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{15d327cf-89c3-4032-9ded-774ae6b0...	REG_BINARY	01 10 08 00 cc cc cc cc c8 02 00 00 00 00 00 00 00 00...
{17043d46-fac2-4561-bca1-0c7a05e95...	REG_BINARY	01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{2db25e6c-f07a-44f4-b6c8-50a330d27...	REG_BINARY	01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{2dd96961-5757-434f-b617-34e732517...	REG_BINARY	01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{3180114b-8338-4740-9a16-444134ad6...	REG_BINARY	01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{3697a558-3ed3-49be-a4c1-c1a444865...	REG_BINARY	01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{375fb39b-08c6-40f2-bdf2-08fa63f970...	REG_BINARY	01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{3a90a266-1519-4d23-911b-e84cd0f02...	REG_BINARY	01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{4137b143-2770-43d4-91a2-55bb0a06...	REG_BINARY	01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{4d9581d2-aef8-4993-84cd-b986ced8...	REG_BINARY	01 10 08 00 cc cc cc cc a0 01 00 00 00 00 00 00 00 00...
{4e718c57-c397-4221-9fbb-14fd51701...	REG_BINARY	01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{567d3836-3f5b-4067-b9c4-952f67701...	REG_BINARY	01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{5b0cb2e2-ab87-4974-9f1c-2f22a654e...	REG_BINARY	01 10 08 00 cc cc cc cc a0 01 00 00 00 00 00 00 00 00...
{64e55933-15a5-495d-a928-ccca43d44...	REG_BINARY	01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{70694559-714a-4a38-a0cd-51439e06f...	REG_BINARY	01 10 08 00 cc cc cc cc 70 03 00 00 00 00 00 00 00 00...
{716b48eb-0a35-4a76-92ab-1d987230...	REG_BINARY	01 10 08 00 cc cc cc cc d0 01 00 00 00 00 00 00 00 0...
{84750a0c-b836-48e3-ab80-104985c85...	REG_BINARY	01 10 08 00 cc cc cc cc f0 02 00 00 00 00 00 00 00 00...
{89a89b7c-b5ab-4ed6-bf05-d3059281...	REG_BINARY	01 10 08 00 cc cc cc cc f0 02 00 00 00 00 00 00 00 00...
{8b50e2ec-7cF0-4b71-b42e-5b0536f6c...	REG_BINARY	01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{916c0dbf-7cec-40f9-9dd9-a5e68b904...	REG_BINARY	01 10 08 00 cc cc cc cc c8 02 00 00 00 00 00 00 00 00...
{91ffecf0-0a9e-4572-95f1-a7111af8696...	REG_BINARY	01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{935b7f48-0ede-44dd-9bc2-e00bb635...	REG_BINARY	01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{941dad9d-7b1a-4354-997b-00cf1aa9...	REG_BINARY	01 10 08 00 cc cc cc cc 98 01 00 00 00 00 00 00 00 00...
{a47525e2-725b-4888-8af1-ba5a60c04...	REG_BINARY	01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{b02a4013-b6b5-4859-9168-1e3299e4...	REG_BINARY	01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{b6b2ca61-fb98-4422-adc2-e7cf56b36...	REG_BINARY	01 10 08 00 cc cc cc cc a0 01 00 00 00 00 00 00 00 00...
{b6fdab6b-dcc6-43e3-99ce-7aeca650...	REG_BINARY	01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{b98b75dc-17c0-4e84-bd4e-2080527c...	REG_BINARY	01 10 08 00 cc cc cc cc f0 02 00 00 00 00 00 00 00 00...
{be7cbdf4-b192-4aa5-94f8-1fb5c5ee0...	REG_BINARY	01 10 08 00 cc cc cc cc a0 01 00 00 00 00 00 00 00 00...
{c016105c-eb34-4519-a5fd-5f4e4ad4d...	REG_BINARY	01 10 08 00 cc cc cc cc 78 01 00 00 00 00 00 00 00 00...
{c42f1cd6-3a95-4ae2-a513-793c3ae61...	REG_BINARY	01 10 08 00 cc cc cc cc d8 01 00 00 00 00 00 00 00 0...
{d5206d58-48e9-11ee-9228-dc7196d9...		

#> Each filter assigned a UUID “key” on creation

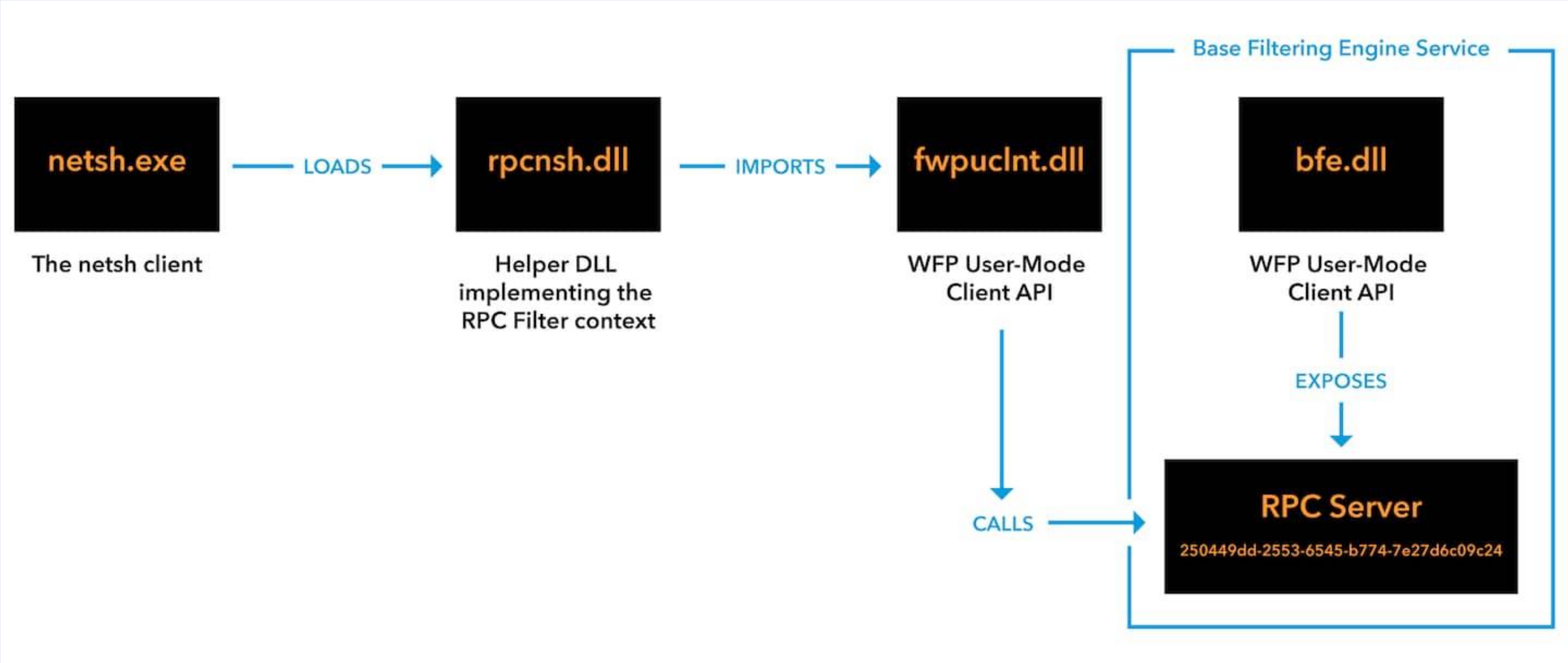
#> Where are filters stored → the Registry!

> *HKLM\SYSTEM\CurrentControlSet\Services\BFE\Parameters\Policy\Persistent\Filter*

#> Stored in binary format:

https://blog.quarkslab.com/windows-filtering-platform-persistent-state-under-the-hood.html

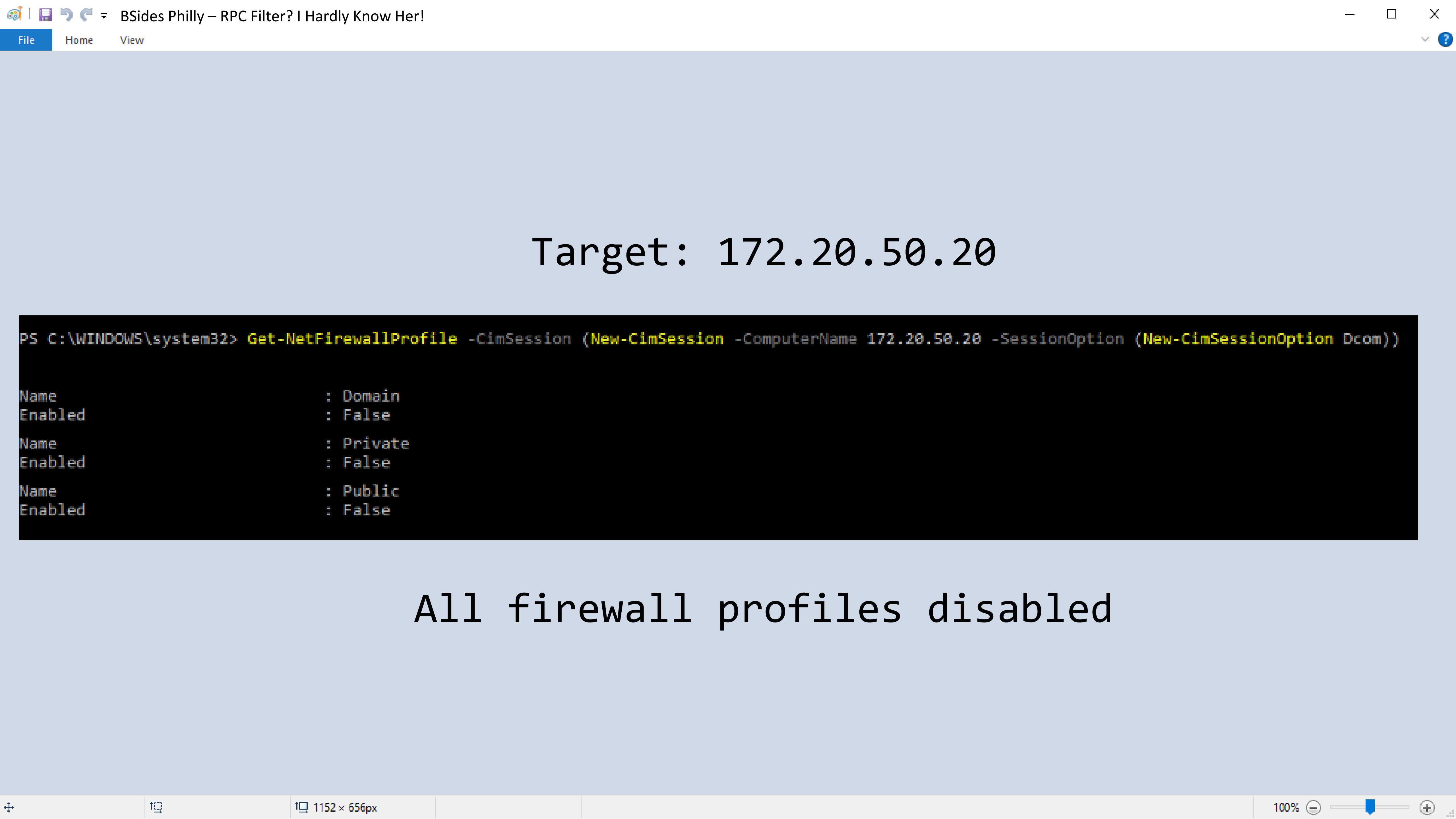
BSides Philly – RPC Filter? I Hardly Know Her!



https://www.akamai.com/blog/security/guide-rpc-filter

```
#> cls
#> echo %SECTION%
```

DEMO
CREATE RPC FILTER VIA NETSH

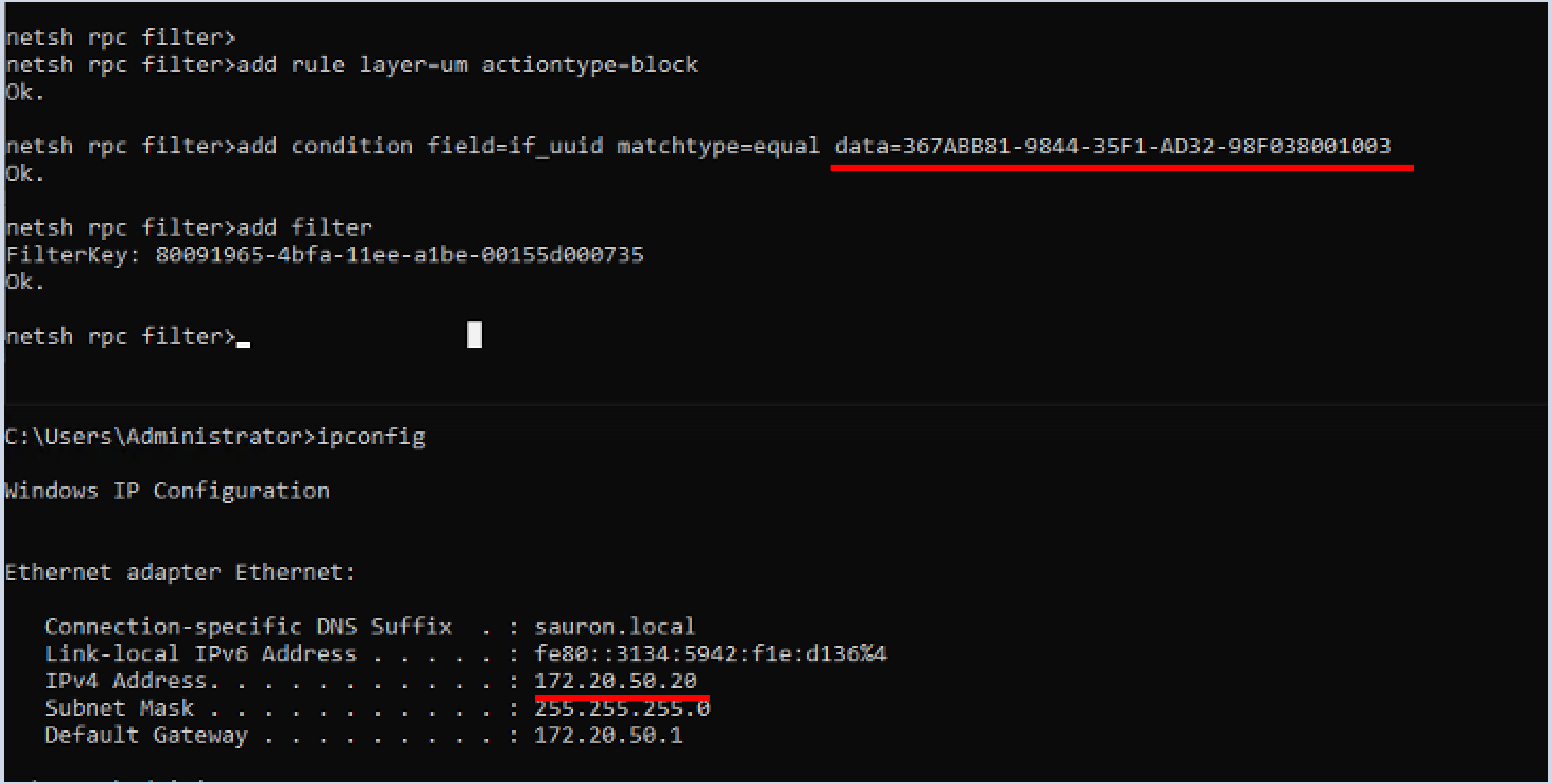


Target: 172.20.50.20

```
PS C:\WINDOWS\system32> Get-NetFirewallProfile -CimSession (New-CimSession -ComputerName 172.20.50.20 -SessionOption (New-CimSessionOption Dcom))


Name                             : Domain
Enabled                          : False

Name                             : Private
Enabled                          : False

Name                             : Public
Enabled                          : False
```

All firewall profiles disabled

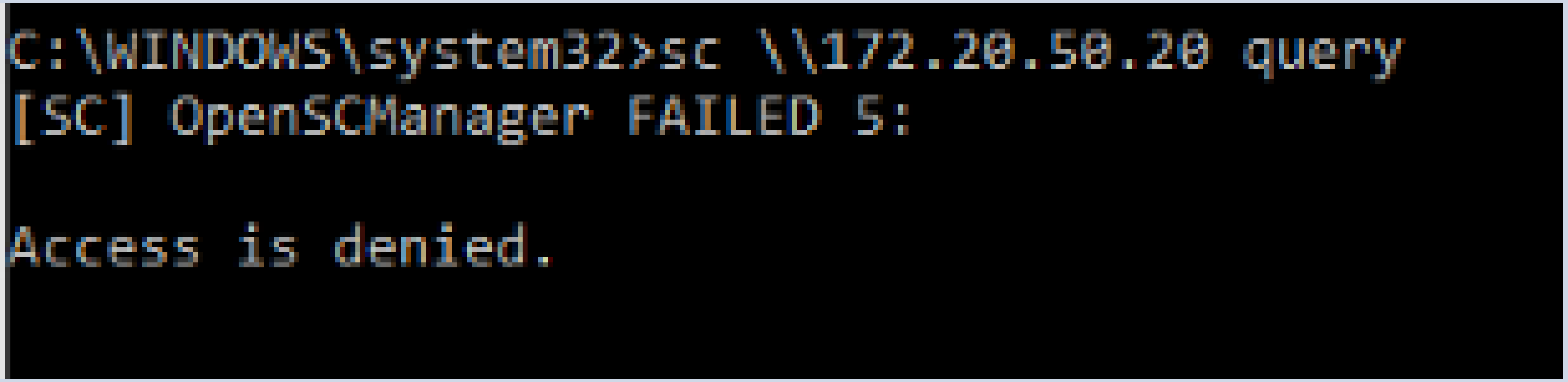
Set rule to block Service Control Manager



```
netsh rpc filter>
netsh rpc filter>add rule layer=um actiontype=block
Ok.

netsh rpc filter>add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32-98F038001003
Ok.

netsh rpc filter>add filter
FilterKey: 80091965-4bfa-11ee-a1be-00155d000735
Ok.

netsh rpc filter>_
```

```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : sauron.local
   Link-local IPv6 Address . . . . . : fe80::3134:5942:f1e:d136%4
   IPv4 Address. . . . . . . . . . . : 172.20.50.20
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.20.50.1
```

sc.exe against target → blocked



```
C:\WINDOWS\system32>sc \\172.20.50.20 query
[SC] OpenSCManager FAILED 5:

Access is denied.
```

```
#> cls
#> echo %SECTION%
```

PAST DEFENSIVE USES

```
#> Microsoft MS08-067 “workaround”

     > add condition
         field=if_uuid
         matchtype=equal
         data=4b324fc8-1670-01d3-1278-5a47bf6ee188

#> Blocks the Server Service RPC interface

#> https://learn.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067
```

#> Previous Works

MSRPC to ATT&CK
https://github.com/jsecurity101/MSRPC-to-ATTACK

Akamai Research
https://www.akamai.com/blog/security-research
https://github.com/akamai/akamai-security-research

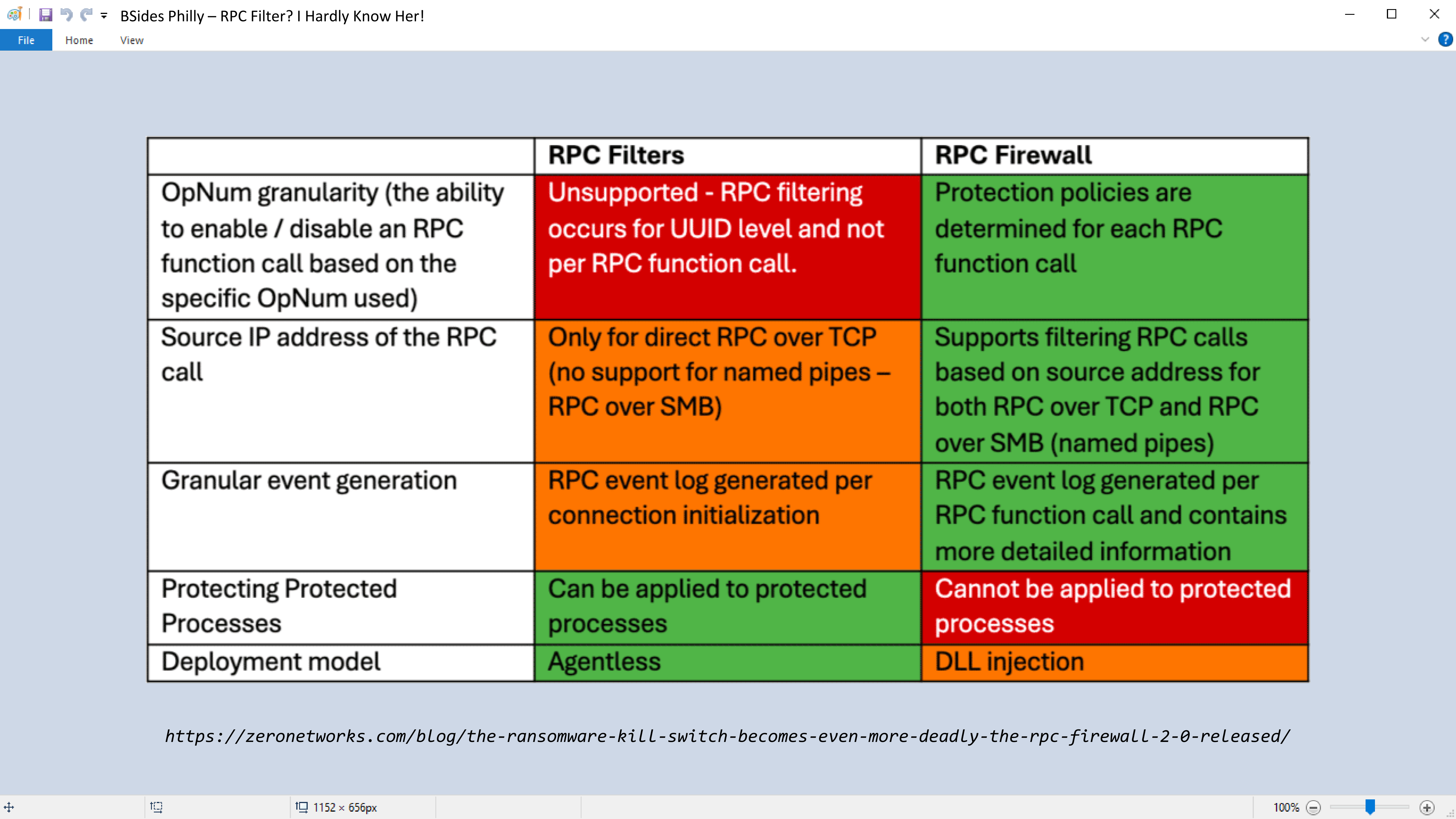
RPC Firewall
https://github.com/zeronetworks/rpcfirewall

#> RPC Firewall by Zero Networks

#> OSS security tool

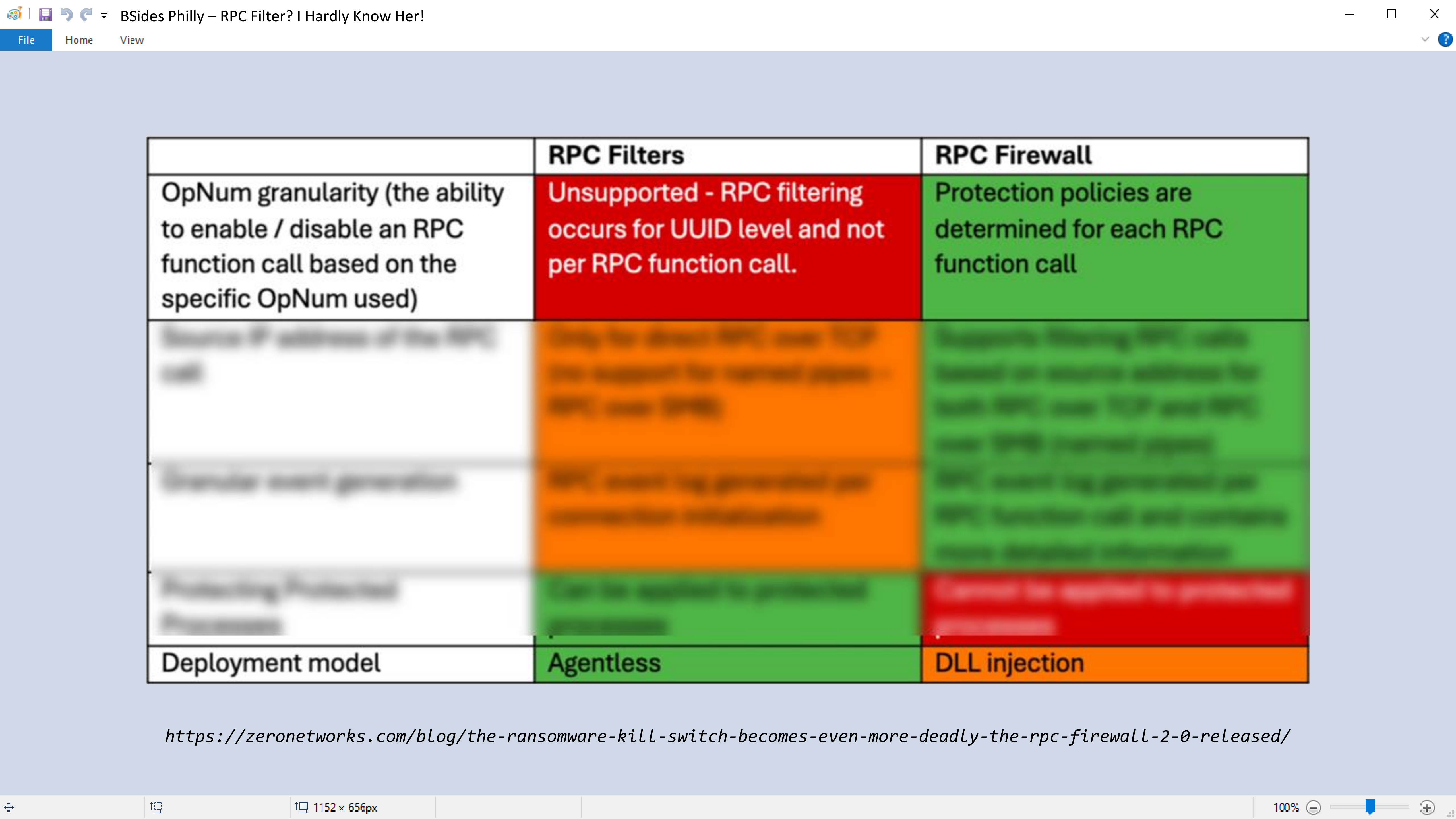
#> Better than RPC Filters if agent-based is okay

#> Solves the all-or-nothing issue



	RPC Filters	RPC Firewall
OpNum granularity (the ability to enable / disable an RPC function call based on the specific OpNum used)	Unsupported - RPC filtering occurs for UUID level and not per RPC function call.	Protection policies are determined for each RPC function call
Source IP address of the RPC call	Only for direct RPC over TCP (no support for named pipes – RPC over SMB)	Supports filtering RPC calls based on source address for both RPC over TCP and RPC over SMB (named pipes)
Granular event generation	RPC event log generated per connection initialization	RPC event log generated per RPC function call and contains more detailed information
Protecting Protected Processes	Can be applied to protected processes	Cannot be applied to protected processes
Deployment model	Agentless	DLL injection

https://zeronetworks.com/blog/the-ransomware-kill-switch-becomes-even-more-deadly-the-rpc-firewall-2-0-released/



	RPC Filters	RPC Firewall
OpNum granularity (the ability to enable / disable an RPC function call based on the specific OpNum used)	Unsupported - RPC filtering occurs for UUID level and not per RPC function call.	Protection policies are determined for each RPC function call
Source IP address of the RPC call	Only for direct RPC over TCP (no support for named pipes - RPC over SMB)	Supports filtering RPC calls based on source address for both RPC over TCP and RPC over SMB (named pipes)
Granular event generation	RPC event log generated per connection initialization	RPC event log generated per RPC function call and contains more detailed information
Protecting Protected Processes	Can be applied to protected processes	Cannot be applied to protected processes
Deployment model	Agentless	DLL injection

https://zeronetworks.com/blog/the-ransomware-kill-switch-becomes-even-more-deadly-the-rpc-firewall-2-0-released/

```
#> cls
#> echo %SECTION%
```

IMPLEMENTATION DETAILS

```
#> Goal: prevent lateral movement attacks

          by

          using RPC Filters across estate
```

```
#> Hurdle 1: If applied, how to track?

#> Solution: Use block + permit/audit trick
#> cls
#> echo %SECTION%
```

AUDITING

#> The issue with blocking: auditing

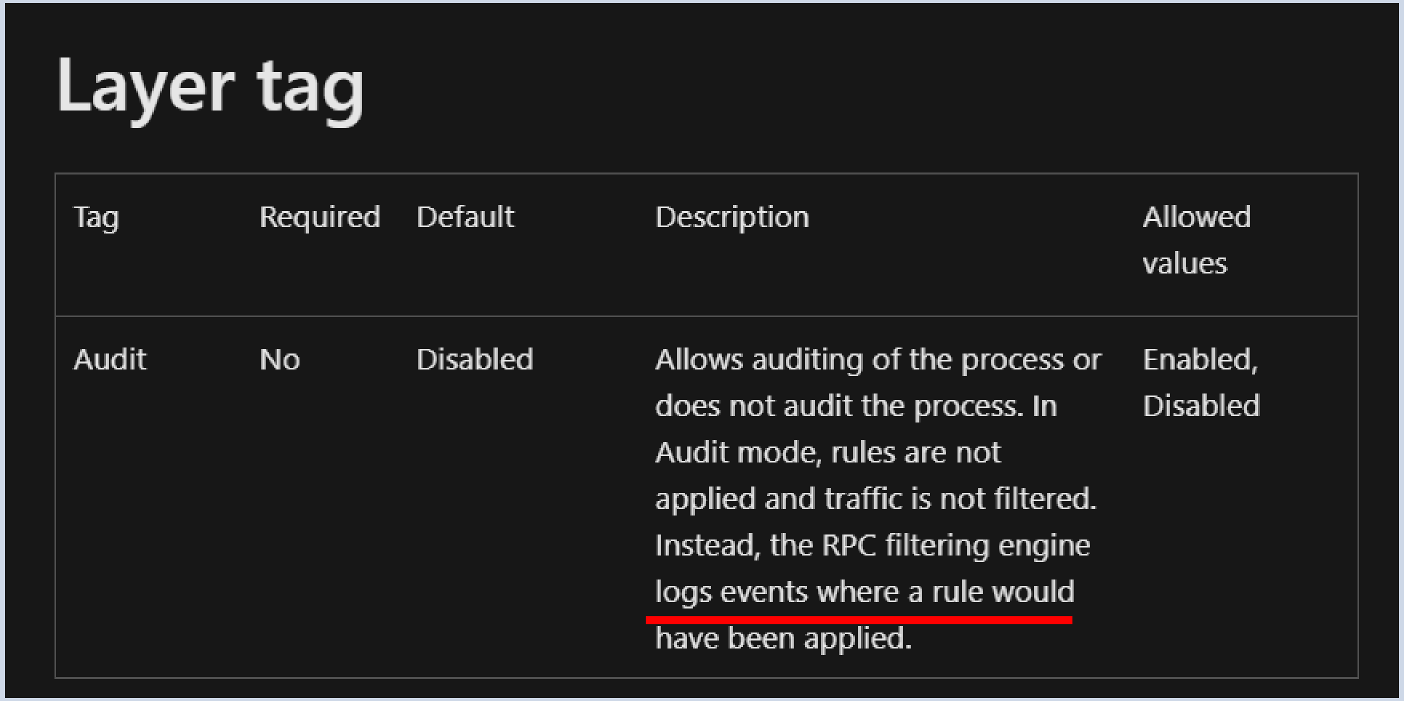
#> Can you even audit RPC filtering activity?

```
#> type 5712.evtx
```

A Remote Procedure Call (RPC) was attempted

“It appears that this event never occurs”
-- Microsoft, creator of Windows (TechNet)

but…



Layer tag

Tag	Required	Default	Description	Allowed values
Audit	No	Disabled	Allows auditing of the process or does not audit the process. In Audit mode, rules are not applied and traffic is not filtered. Instead, the RPC filtering engine logs events where a rule would have been applied.	Enabled, Disabled

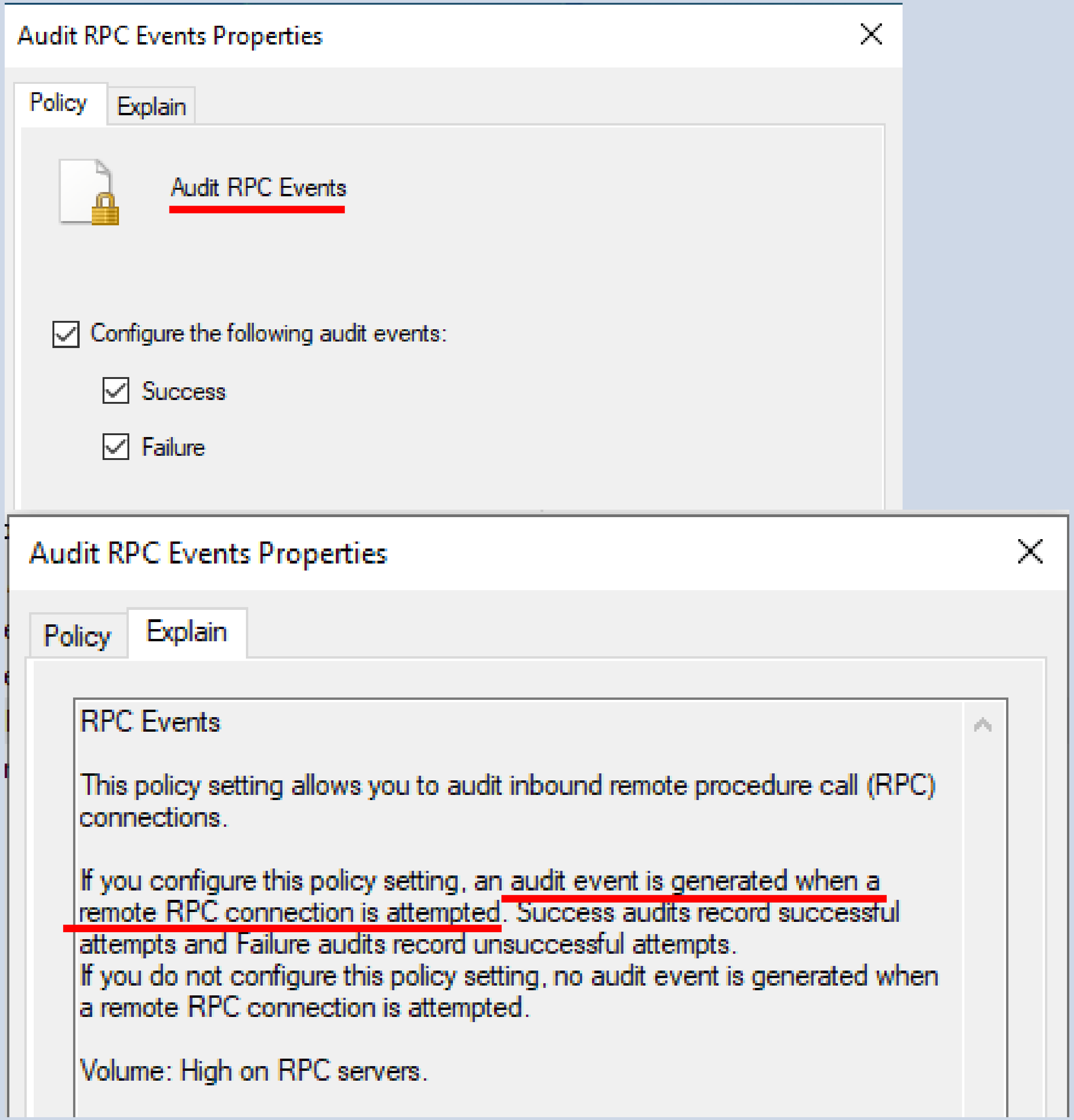
https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc730626(v=ws.10)

netsh documentation

- filters can be audited
- auditing is apparently logged
- probably in Event log or ETW

BSides Philly – RPC Filter? I Hardly Know Her!

File Home View



Audit RPC Events Properties

Audit RPC Events

☑ Configure the following audit events:

☑ Success

☑ Failure

Audit RPC Events Properties

RPC Events

This policy setting allows you to audit inbound remote procedure call (RPC) connections.

If you configure this policy setting, an audit event is generated when a remote RPC connection is attempted. Success audits record successful attempts and Failure audits record unsuccessful attempts.
If you do not configure this policy setting, no audit event is generated when a remote RPC connection is attempted.

Volume: High on RPC servers.

Advanced Audit GPO

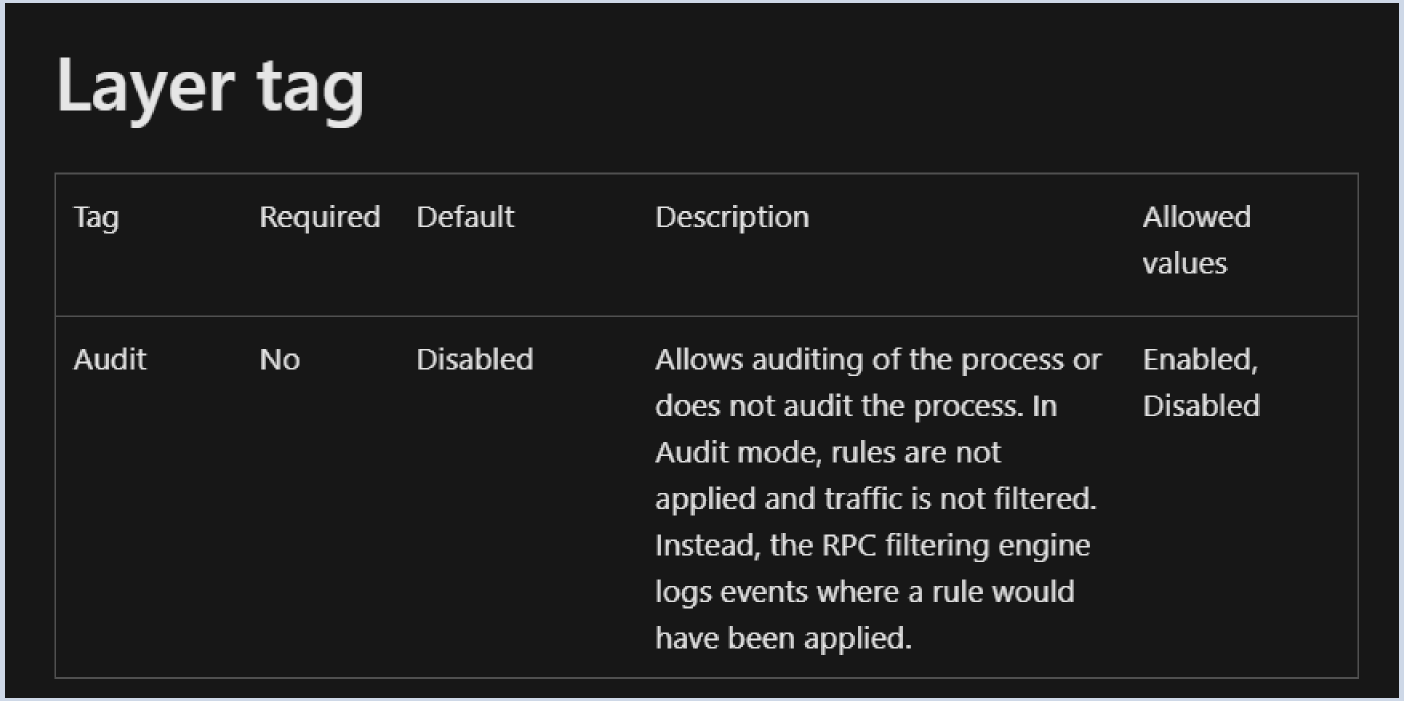
- RPC connections can be audited
- likely in Event log, like most Adv. Audit

1152 × 656px 100%

BSides Philly – RPC Filter? I Hardly Know Her!

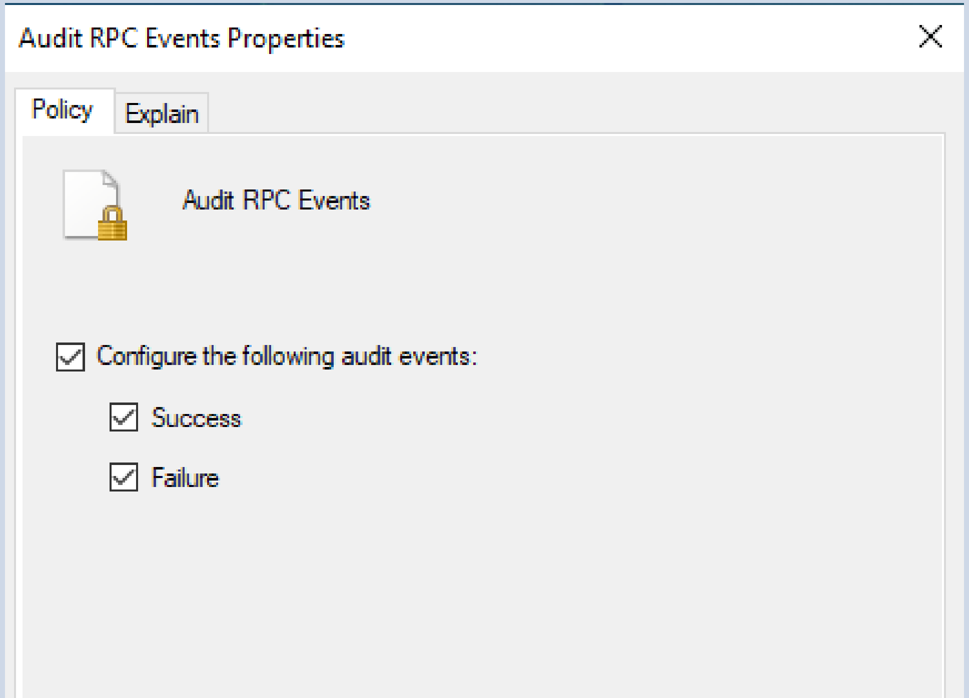
File Home View

Adv. Audit + Audited Filter



Layer tag

Tag	Required	Default	Description	Allowed values
Audit	No	Disabled	Allows auditing of the process or does not audit the process. In Audit mode, rules are not applied and traffic is not filtered. Instead, the RPC filtering engine logs events where a rule would have been applied.	Enabled, Disabled



Audit RPC Events Properties

Audit RPC Events

☑ Configure the following audit events:

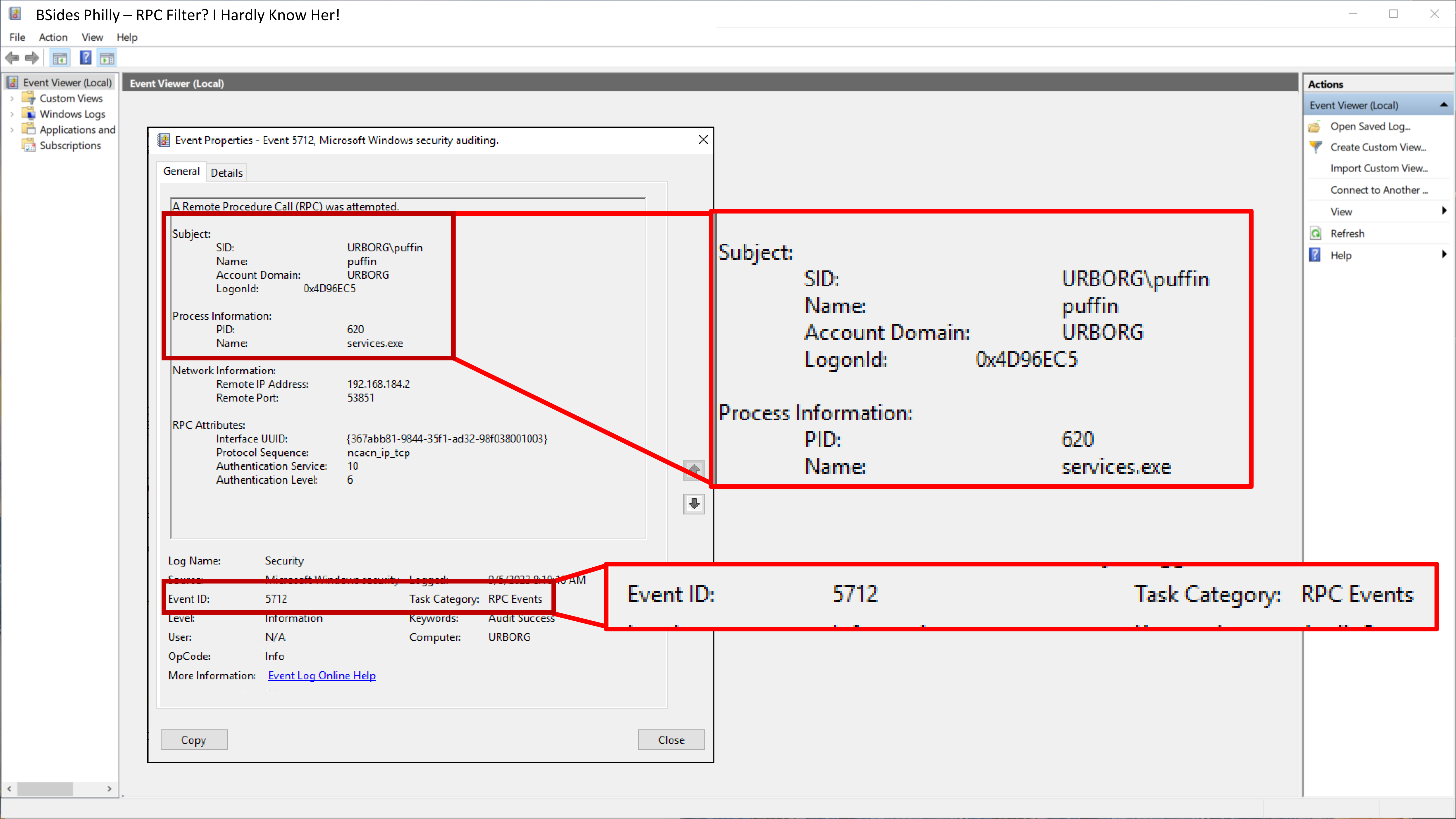
☑ Success

☑ Failure

=

1152 × 656px

100%



Event Properties - Event 5712, Microsoft Windows security auditing.

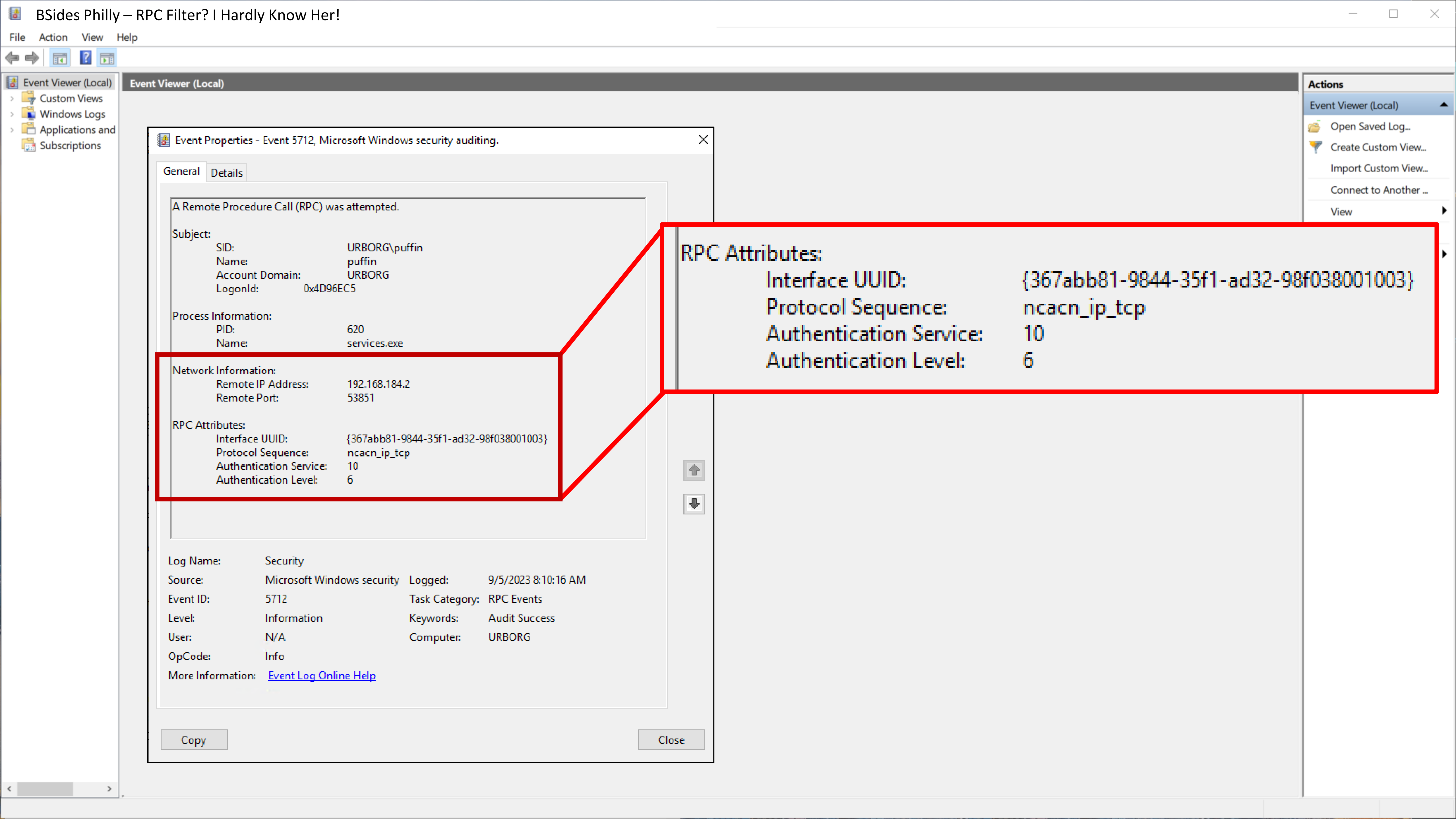
```
A Remote Procedure Call (RPC) was attempted.

Subject:
        SID:                    URBORG\puffin
        Name:                   puffin
        Account Domain:         URBORG
        LogonId:        0x4D96EC5

Process Information:
        PID:                    620
        Name:                   services.exe

Network Information:
        Remote IP Address:      192.168.184.2
        Remote Port:            53851

RPC Attributes:
        Interface UUID:         {367abb81-9844-35f1-ad32-98f038001003}
        Protocol Sequence:      ncacn_ip_tcp
        Authentication Service: 10
        Authentication Level:   6
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          9/5/2023 8:10:15 AM
Event ID:          5712                         Task Category:   RPC Events
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        URBORG
OpCode:            Info
More Information:  Event Log Online Help
```

Subject:
SID: URBORG\puffin
Name: puffin
Account Domain: URBORG
LogonId: 0x4D96EC5

Process Information:
PID: 620
Name: services.exe

Event ID: 5712 Task Category: RPC Events



```
A Remote Procedure Call (RPC) was attempted.

Subject:
        SID:                    URBORG\puffin
        Name:                   puffin
        Account Domain:         URBORG
        LogonId:        0x4D96EC5

Process Information:
        PID:                    620
        Name:                   services.exe

Network Information:
        Remote IP Address:      192.168.184.2
        Remote Port:            53851

RPC Attributes:
        Interface UUID:         {367abb81-9844-35f1-ad32-98f038001003}
        Protocol Sequence:      ncacn_ip_tcp
        Authentication Service: 10
        Authentication Level:   6
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	9/5/2023 8:10:16 AM
Event ID:	5712	Task Category:	RPC Events
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	URBORG
OpCode:	Info		
More Information:	Event Log Online Help		

```
RPC Attributes:
        Interface UUID:         {367abb81-9844-35f1-ad32-98f038001003}
        Protocol Sequence:      ncacn_ip_tcp
        Authentication Service: 10
        Authentication Level:   6
```

```
CMD>
  netsh> add rule layer=um actiontype=block
         audit=enable

  -->    ERROR!


#> audit=enable MUST have actiontype=permit

#> can’t audit blocks
#> what if you duplicate rules?

CMD>
  netsh> add rule actiontype=block
  netsh> add rule actiontype=permit audit=enable


#> blocked connections are now logged!


(order doesn’t seem to matter)
```

```
#> Hurdle 2: How to deploy?

#> Solutions:

      > Registry only via GPP
      > netsh.exe via GPO Startup Script
      > One of the above w/ another tool (e.g. SCCM)
      > Pre-deployed in golden image
```

#> netsh.exe method

> Rules can be stored in a file (-f option)
> Can store on write-restricted share

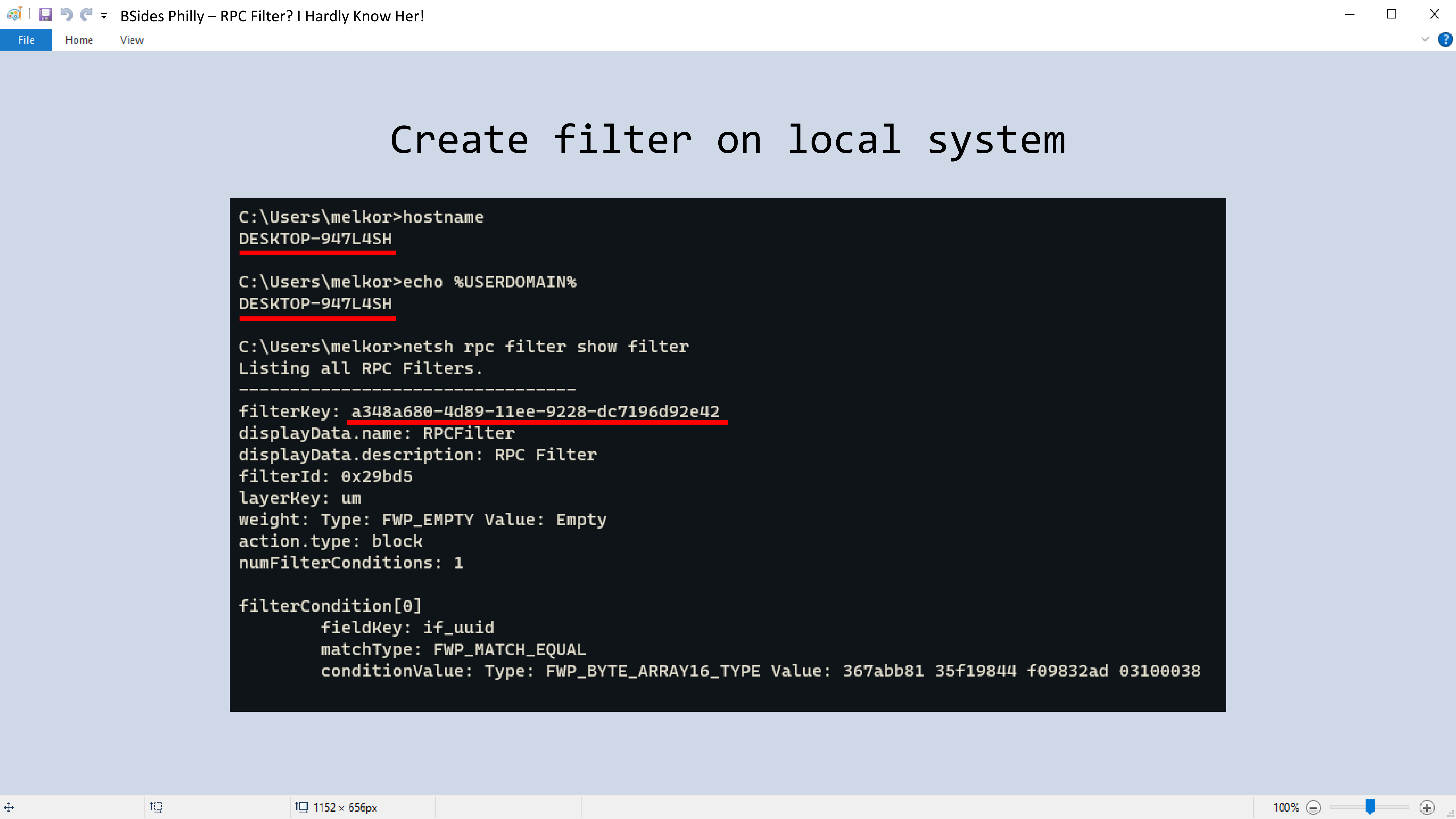
#> Registry method

> Requires restart after applying

```
#> Filter keys can be set on creation

#> Allows consistent management for
   transitioning from audit → blocking
```

```
#> cls
#> echo %SECTION%
```

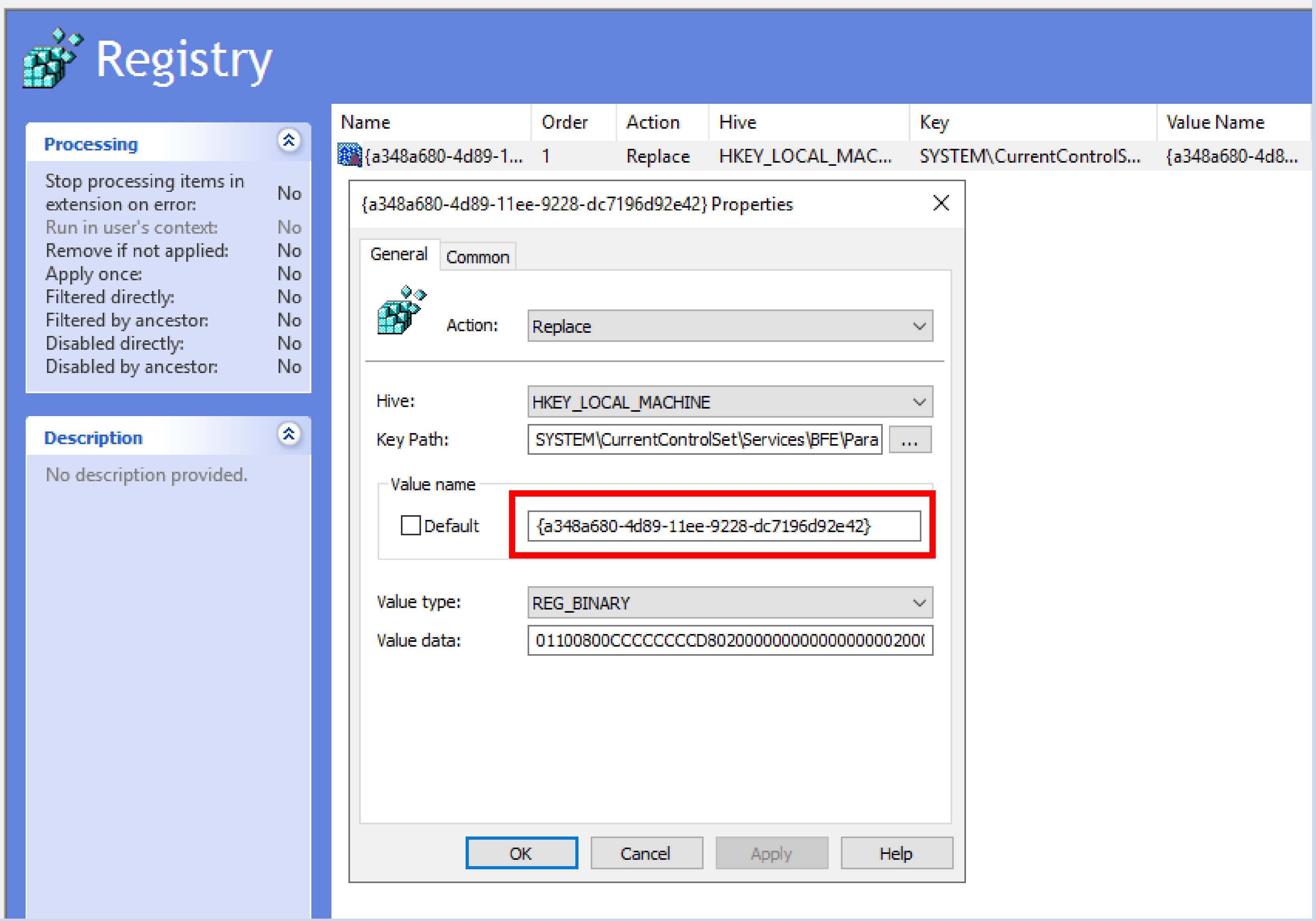
DEMO
SET FILTER VIA REGISTRY GPP



Create filter on local system

```
C:\Users\melkor>hostname
DESKTOP-947L4SH

C:\Users\melkor>echo %USERDOMAIN%
DESKTOP-947L4SH

C:\Users\melkor>netsh rpc filter show filter
Listing all RPC Filters.
---------------------------------
filterKey: a348a680-4d89-11ee-9228-dc7196d92e42
displayData.name: RPCFilter
displayData.description: RPC Filter
filterId: 0x29bd5
layerKey: um
weight: Type: FWP_EMPTY Value: Empty
action.type: block
numFilterConditions: 1

filterCondition[0]
        fieldKey: if_uuid
        matchType: FWP_MATCH_EQUAL
        conditionValue: Type: FWP_BYTE_ARRAY16_TYPE Value: 367abb81 35f19844 f09832ad 03100038
```

BSides Philly – RPC Filter? I Hardly Know Her!



Registry

Processing

Stop processing items in extension on error: No
Run in user's context: No
Remove if not applied: No
Apply once: No
Filtered directly: No
Filtered by ancestor: No
Disabled directly: No
Disabled by ancestor: No

Description

No description provided.

Name	Order	Action	Hive	Key	Value Name
{a348a680-4d89-1...	1	Replace	HKEY_LOCAL_MAC...	SYSTEM\CurrentControlS...	{a348a680-4d8...

{a348a680-4d89-11ee-9228-dc7196d92e42} Properties

Action: Replace

Hive: HKEY_LOCAL_MACHINE

Key Path: SYSTEM\CurrentControlSet\Services\BFE\Para

Value name

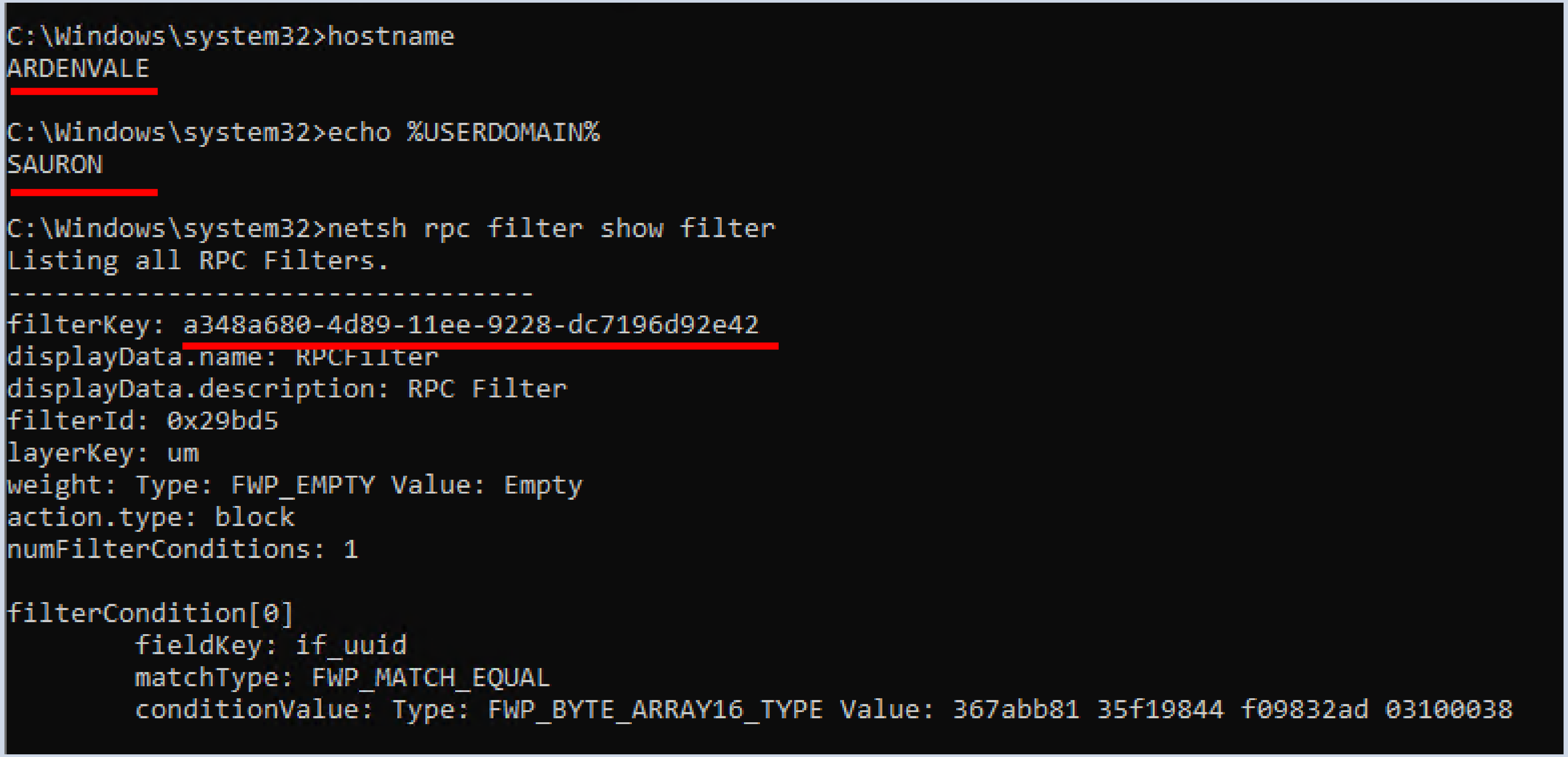
□ Default {a348a680-4d89-11ee-9228-dc7196d92e42}

Value type: REG_BINARY

Value data: 01100800CCCCCCCCD802000000000000000000200(

Deploy via Registry GPP

Check filter on domain system (post-reboot)

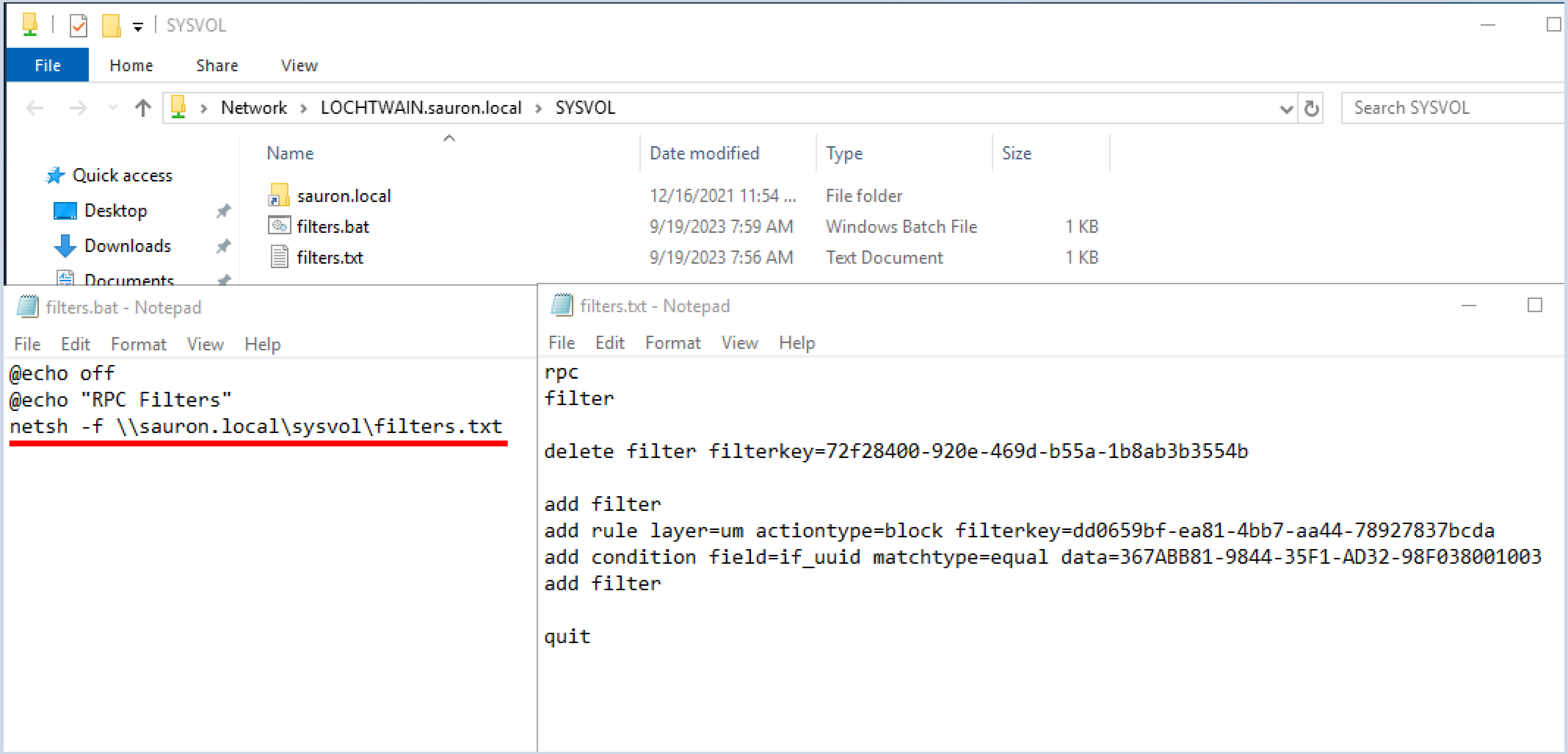


```
C:\Windows\system32>hostname
ARDENVALE

C:\Windows\system32>echo %USERDOMAIN%
SAURON

C:\Windows\system32>netsh rpc filter show filter
Listing all RPC Filters.
-----------------------------------
filterKey: a348a680-4d89-11ee-9228-dc7196d92e42
displayData.name: RPCFilter
displayData.description: RPC Filter
filterId: 0x29bd5
layerKey: um
weight: Type: FWP_EMPTY Value: Empty
action.type: block
numFilterConditions: 1

filterCondition[0]
        fieldKey: if_uuid
        matchType: FWP_MATCH_EQUAL
        conditionValue: Type: FWP_BYTE_ARRAY16_TYPE Value: 367abb81 35f19844 f09832ad 03100038
```

```
#> cls
#> echo %SECTION%
```

DEMO
SET FILTER VIA GPO SCRIPT

Create filters on SYSVOL



Name	Date modified	Type	Size
sauron.local	12/16/2021 11:54 ...	File folder	
filters.bat	9/19/2023 7:59 AM	Windows Batch File	1 KB
filters.txt	9/19/2023 7:56 AM	Text Document	1 KB

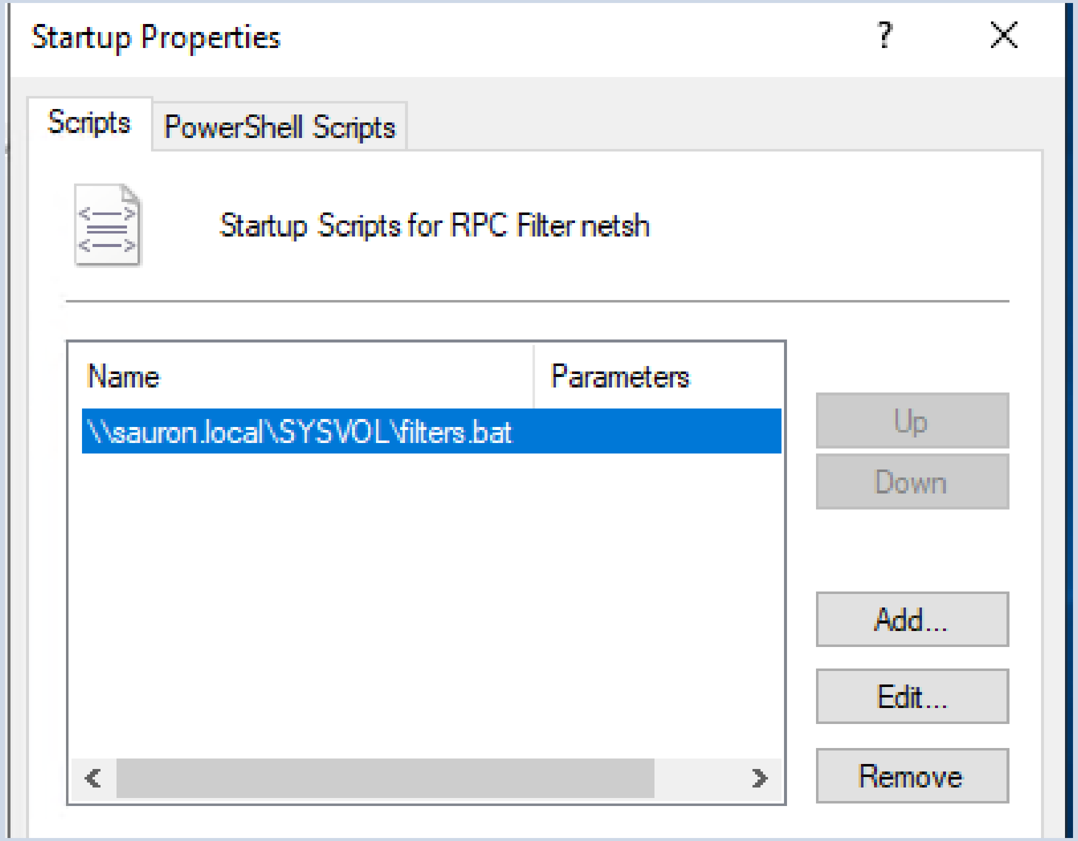
filters.bat

```
@echo off
@echo "RPC Filters"
netsh -f \\sauron.local\sysvol\filters.txt
```

filters.txt

```
rpc
filter

delete filter filterkey=72f28400-920e-469d-b55a-1b8ab3b3554b

add filter
add rule layer=um actiontype=block filterkey=dd0659bf-ea81-4bb7-aa44-78927837bcda
add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32-98F038001003
add filter

quit
```

Create startup script (or scheduled task, etc)



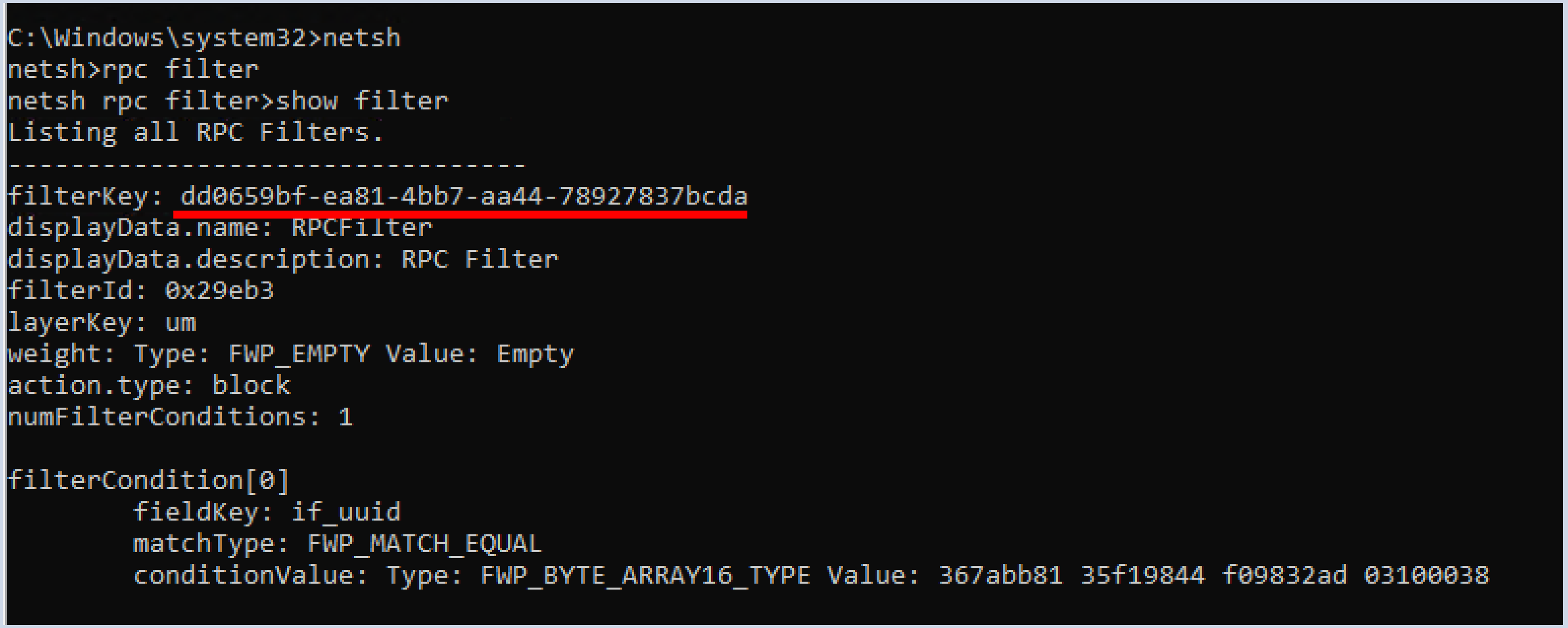
Startup Properties

Scripts | PowerShell Scripts

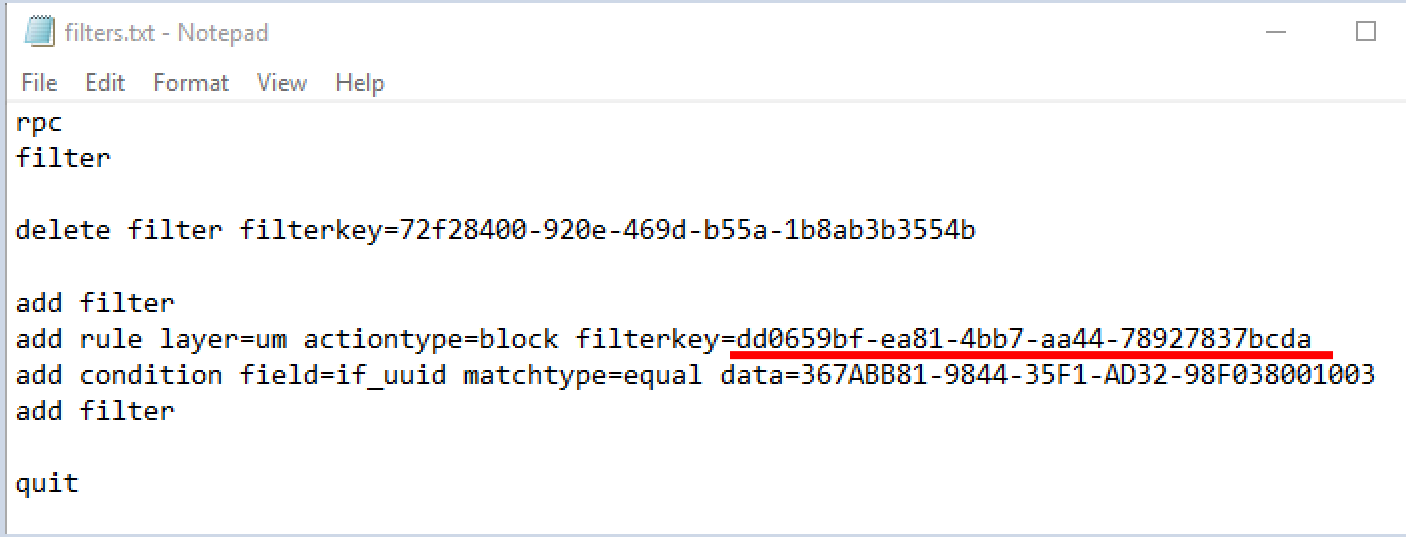
Startup Scripts for RPC Filter netsh

Name	Parameters
\\sauron.local\SYSVOL\filters.bat	

BSides Philly – RPC Filter? I Hardly Know Her!



```
C:\Windows\system32>netsh
netsh>rpc filter
netsh rpc filter>show filter
Listing all RPC Filters.
---------------------------------
filterKey: dd0659bf-ea81-4bb7-aa44-78927837bcda
displayData.name: RPCFilter
displayData.description: RPC Filter
filterId: 0x29eb3
layerKey: um
weight: Type: FWP_EMPTY Value: Empty
action.type: block
numFilterConditions: 1

filterCondition[0]
        fieldKey: if_uuid
        matchType: FWP_MATCH_EQUAL
        conditionValue: Type: FWP_BYTE_ARRAY16_TYPE Value: 367abb81 35f19844 f09832ad 03100038
```



```
rpc
filter

delete filter filterkey=72f28400-920e-469d-b55a-1b8ab3b3554b

add filter
add rule layer=um actiontype=block filterkey=dd0659bf-ea81-4bb7-aa44-78927837bcda
add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32-98F038001003
add filter

quit
```

Filters applied to system

#> Hurdle 3: What about legitimate use?

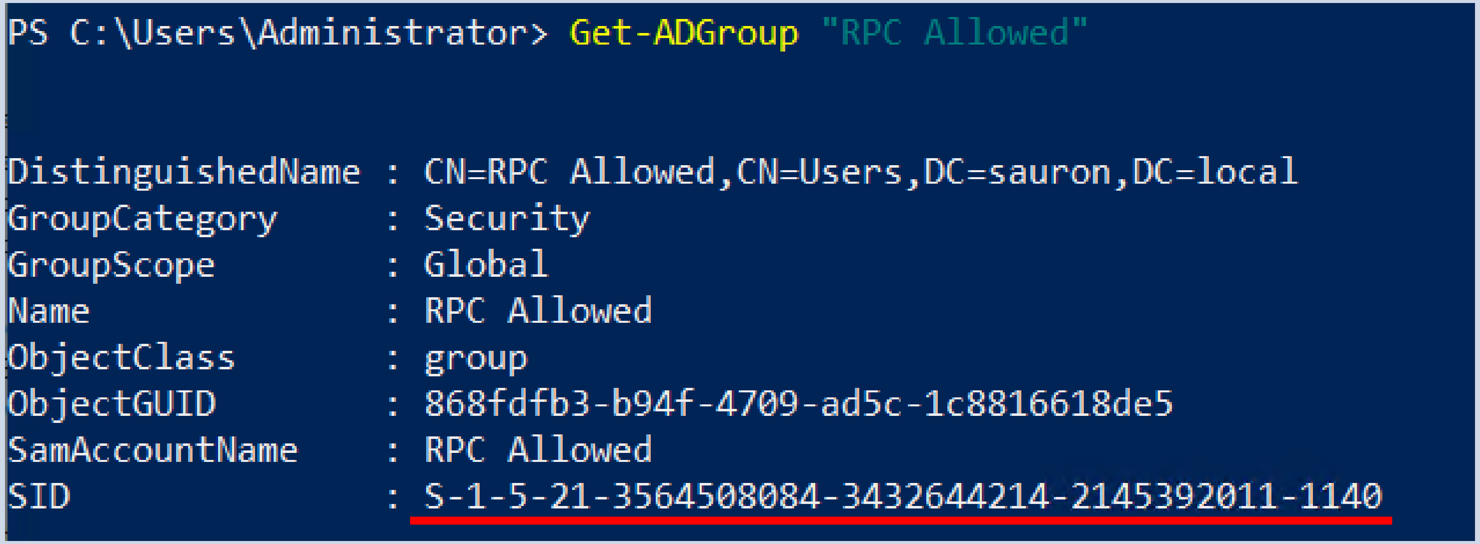
#> Solution: Create domain group then allow via filter

```
#> cls
#> echo %SECTION%
```

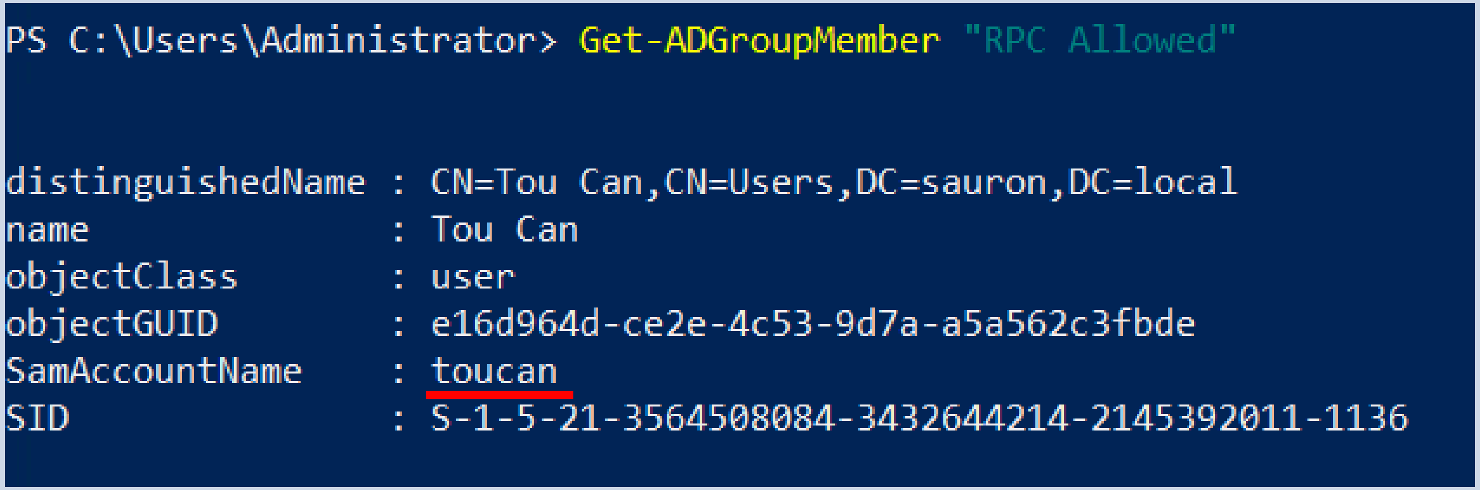
DEMO
FILTER BY DOMAIN GROUP

BSides Philly – RPC Filter? I Hardly Know Her!

File Home View



```
PS C:\Users\Administrator> Get-ADGroup "RPC Allowed"


DistinguishedName : CN=RPC Allowed,CN=Users,DC=sauron,DC=local
GroupCategory     : Security
GroupScope        : Global
Name              : RPC Allowed
ObjectClass       : group
ObjectGUID        : 868fdfb3-b94f-4709-ad5c-1c8816618de5
SamAccountName    : RPC Allowed
SID               : S-1-5-21-3564508084-3432644214-2145392011-1140
```



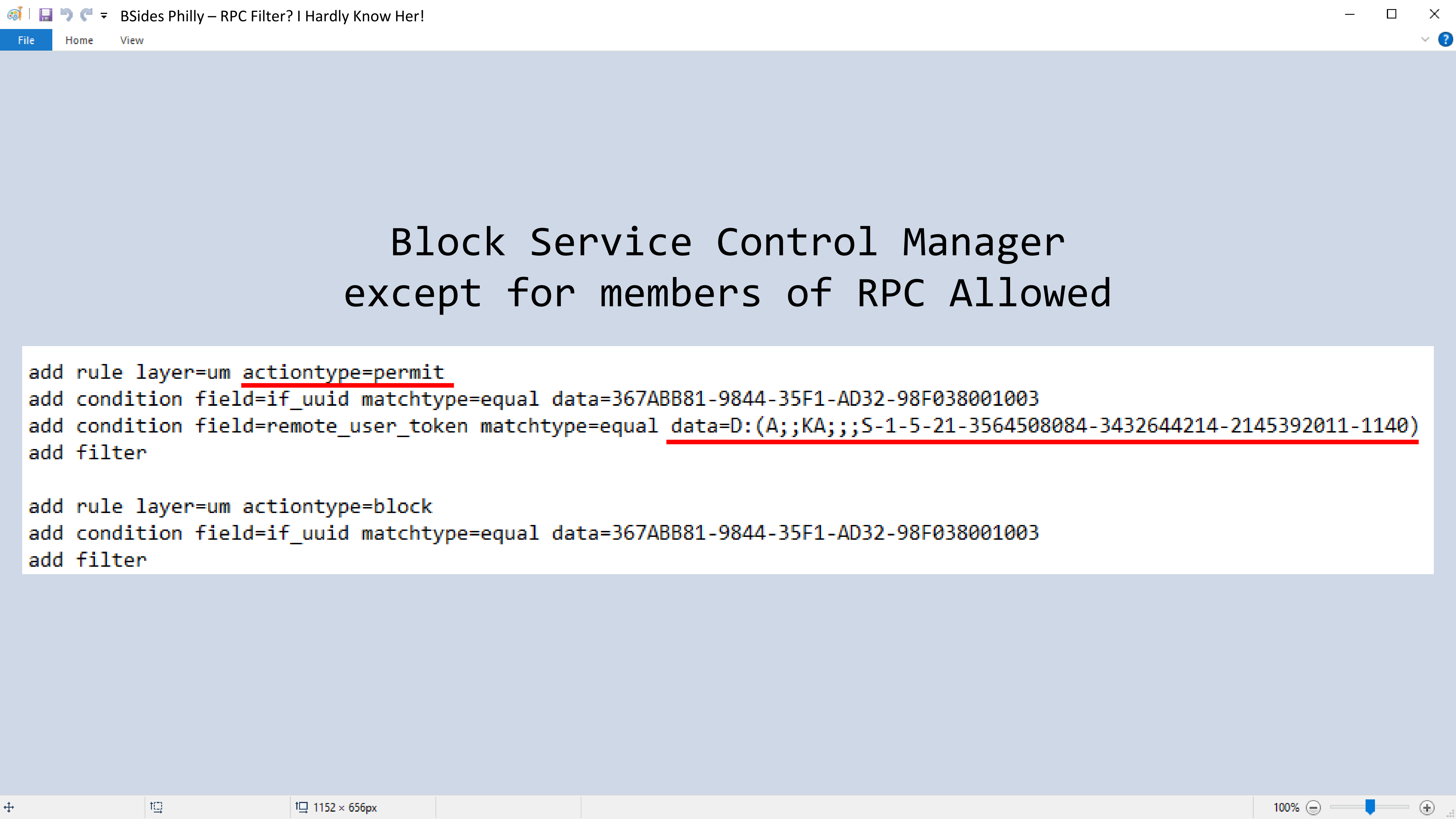
```
PS C:\Users\Administrator> Get-ADGroupMember "RPC Allowed"


distinguishedName : CN=Tou Can,CN=Users,DC=sauron,DC=local
name              : Tou Can
objectClass       : user
objectGUID        : e16d964d-ce2e-4c53-9d7a-a5a562c3fbde
SamAccountName    : toucan
SID               : S-1-5-21-3564508084-3432644214-2145392011-1136
```

AD Group: RPC Allowed

Member: toucan

1152 × 656px

100%



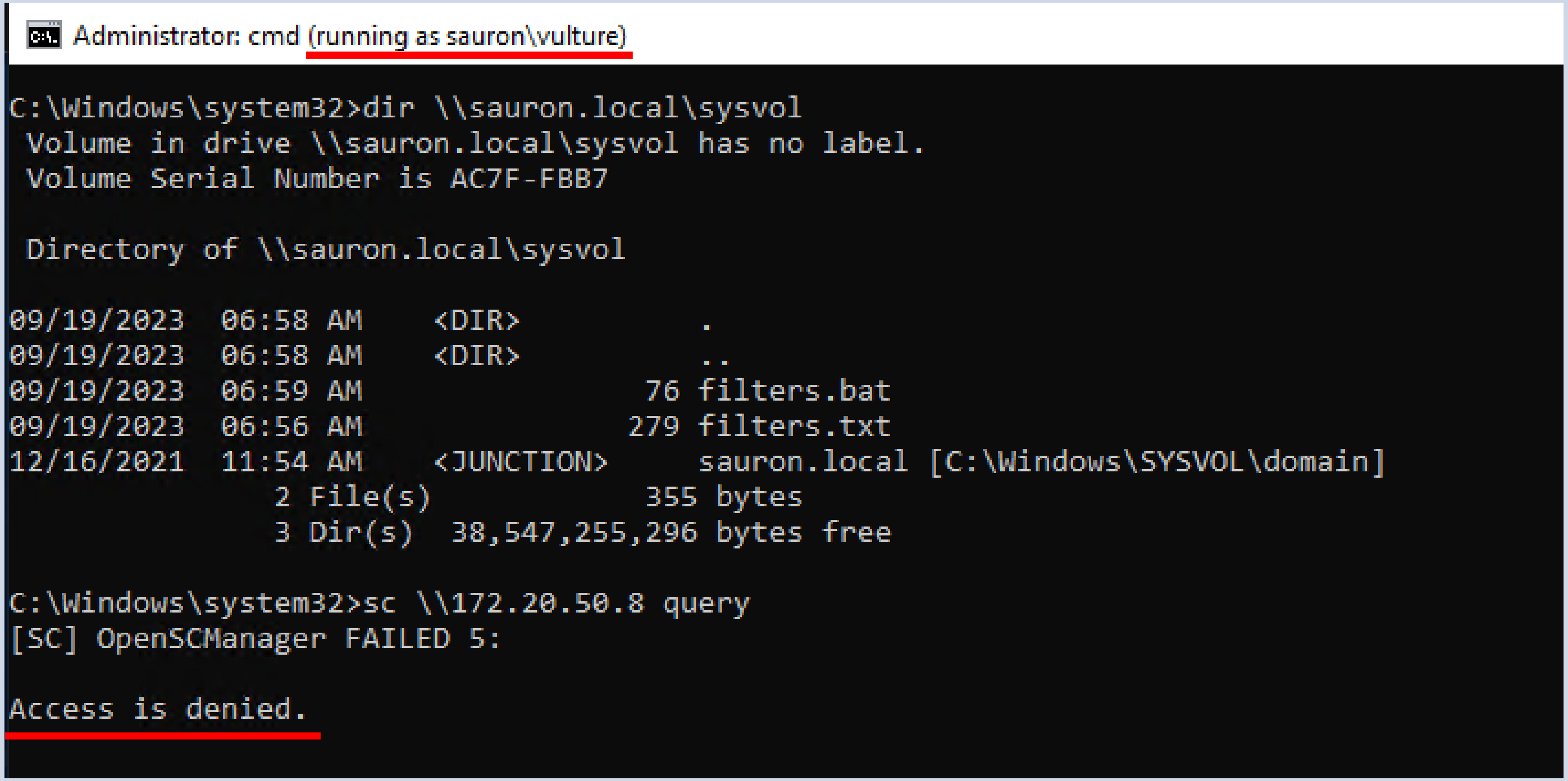
Block Service Control Manager except for members of RPC Allowed

```
add rule layer=um actiontype=permit
add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32-98F038001003
add condition field=remote_user_token matchtype=equal data=D:(A;;KA;;;S-1-5-21-3564508084-3432644214-2145392011-1140)
add filter

add rule layer=um actiontype=block
add condition field=if_uuid matchtype=equal data=367ABB81-9844-35F1-AD32-98F038001003
add filter
```

BSides Philly – RPC Filter? I Hardly Know Her!

File Home View

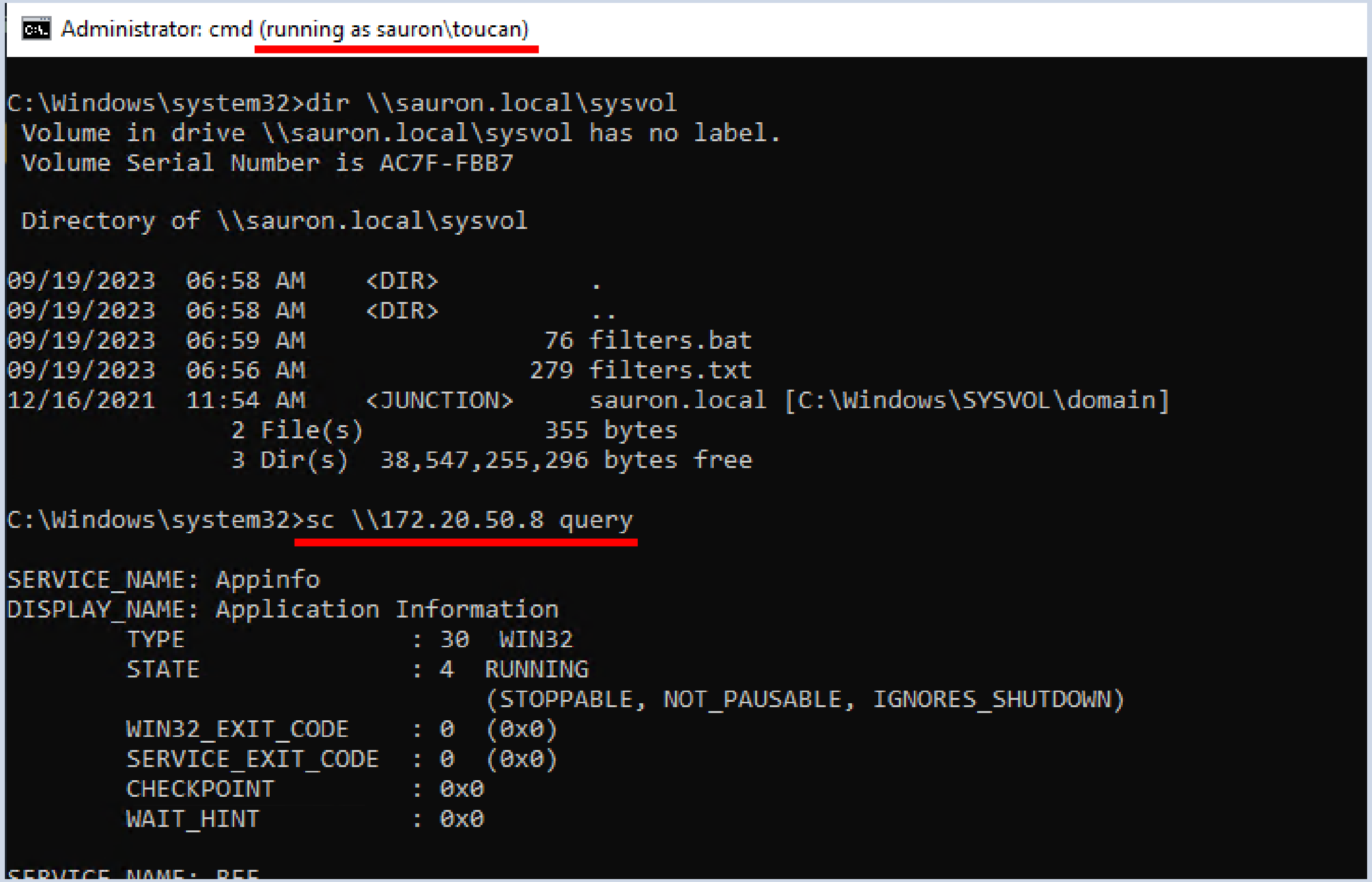
sc.exe blocked for user vulture



```
C:\Windows\system32>dir \\sauron.local\sysvol
 Volume in drive \\sauron.local\sysvol has no label.
 Volume Serial Number is AC7F-FBB7

 Directory of \\sauron.local\sysvol

09/19/2023  06:58 AM    <DIR>          .
09/19/2023  06:58 AM    <DIR>          ..
09/19/2023  06:59 AM                76 filters.bat
09/19/2023  06:56 AM               279 filters.txt
12/16/2021  11:54 AM    <JUNCTION>     sauron.local [C:\Windows\SYSVOL\domain]
               2 File(s)            355 bytes
               3 Dir(s)  38,547,255,296 bytes free

C:\Windows\system32>sc \\172.20.50.8 query
[SC] OpenSCManager FAILED 5:

Access is denied.
```

1152 × 656px 100%

sc.exe allowed for user toucan



Administrator: cmd (running as sauron\toucan)

```
C:\Windows\system32>dir \\sauron.local\sysvol
 Volume in drive \\sauron.local\sysvol has no label.
 Volume Serial Number is AC7F-FBB7

 Directory of \\sauron.local\sysvol

09/19/2023  06:58 AM    <DIR>          .
09/19/2023  06:58 AM    <DIR>          ..
09/19/2023  06:59 AM                76 filters.bat
09/19/2023  06:56 AM               279 filters.txt
12/16/2021  11:54 AM    <JUNCTION>     sauron.local [C:\Windows\SYSVOL\domain]
               2 File(s)            355 bytes
               3 Dir(s)  38,547,255,296 bytes free

C:\Windows\system32>sc \\172.20.50.8 query

SERVICE_NAME: Appinfo
DISPLAY_NAME: Application Information
        TYPE               : 30  WIN32
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

SERVICE_NAME: BFE
```

```
#> cls
#> echo %SECTION%
```

LIMITATIONS

#> Registry-method is a non-starter sometimes

#> Cannot filter on opnum

  > Useful for blocking *specific* actions

#> Hard to know entire impact of blocking

#> Only for remote connections, not local

#> BFE API is local only

#> Local Windows log collection is hard/uncommon

Questions?

𝕏 @2xxeformyshirt
slides
https://github.com/SecurityRiskAdvisors/public-assets