NETSPI™

Into the Abyss: Evaluating Active Directory SMB Shares on Scale

SCOTT SUTHERLAND / SENIOR DIRECTOR, NETSPI

Scott Sutherland

Senior Director, NetSPI

Adversary Simulation &
Infrastructure Testing

Whoami

Twitter	**@_nullbind**
Blogs	https://blog.netspi.com/author/scott-sutherland/
Decks	http://slideshare.net/nullbind
Code	https://github.com/NetSPI/PowerUpSQL https://github.com/NetSPI/SQLC2 https://github.com/NetSPI/ESC https://github.com/NetSPI/PowerHunt https://github.com/NetSPI/PowerHuntShares

PowerUpSQL

EVILSQL CLIENT Esc

Agenda

1 **What's the Problem?**
Why should I care about share access?

2 **Share Permissions Primer**
How do they work and where do things go wrong?

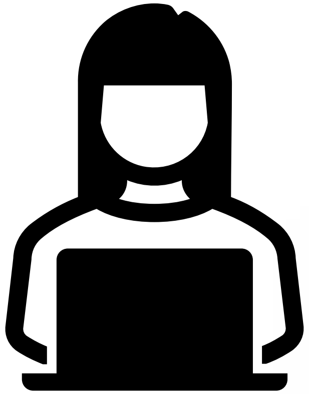
3 **What's the Impact?**
Exploiting SMB share access!

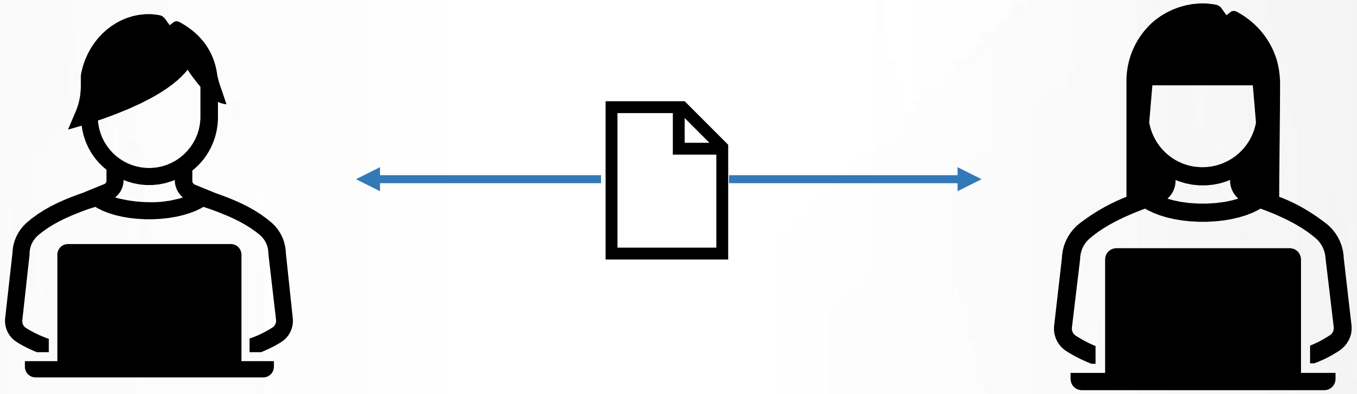
4 **Share Remediation**
How can we streamline share inventory and remediation?

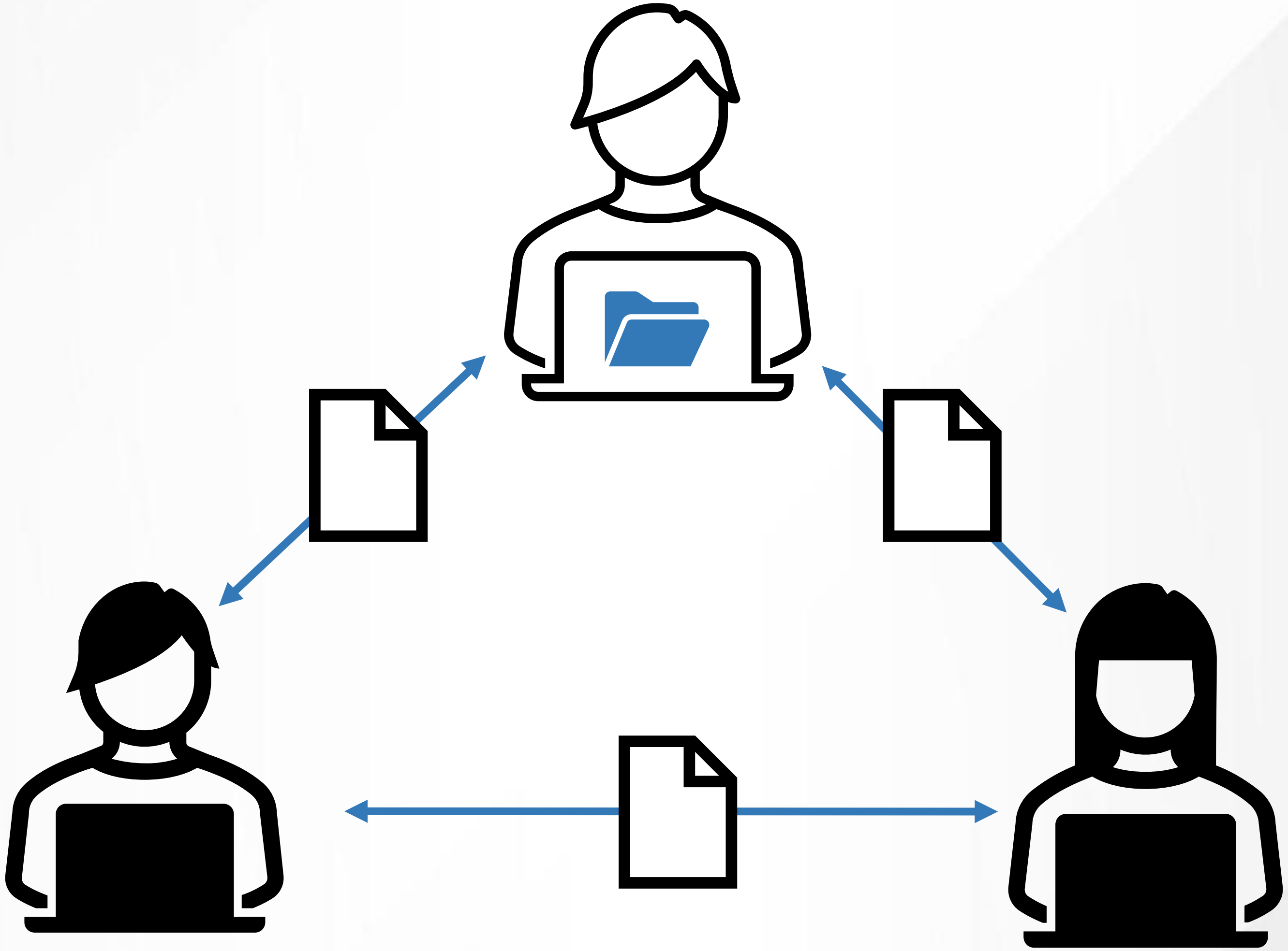
5 **PowerHuntShares**
Let's automate some things!

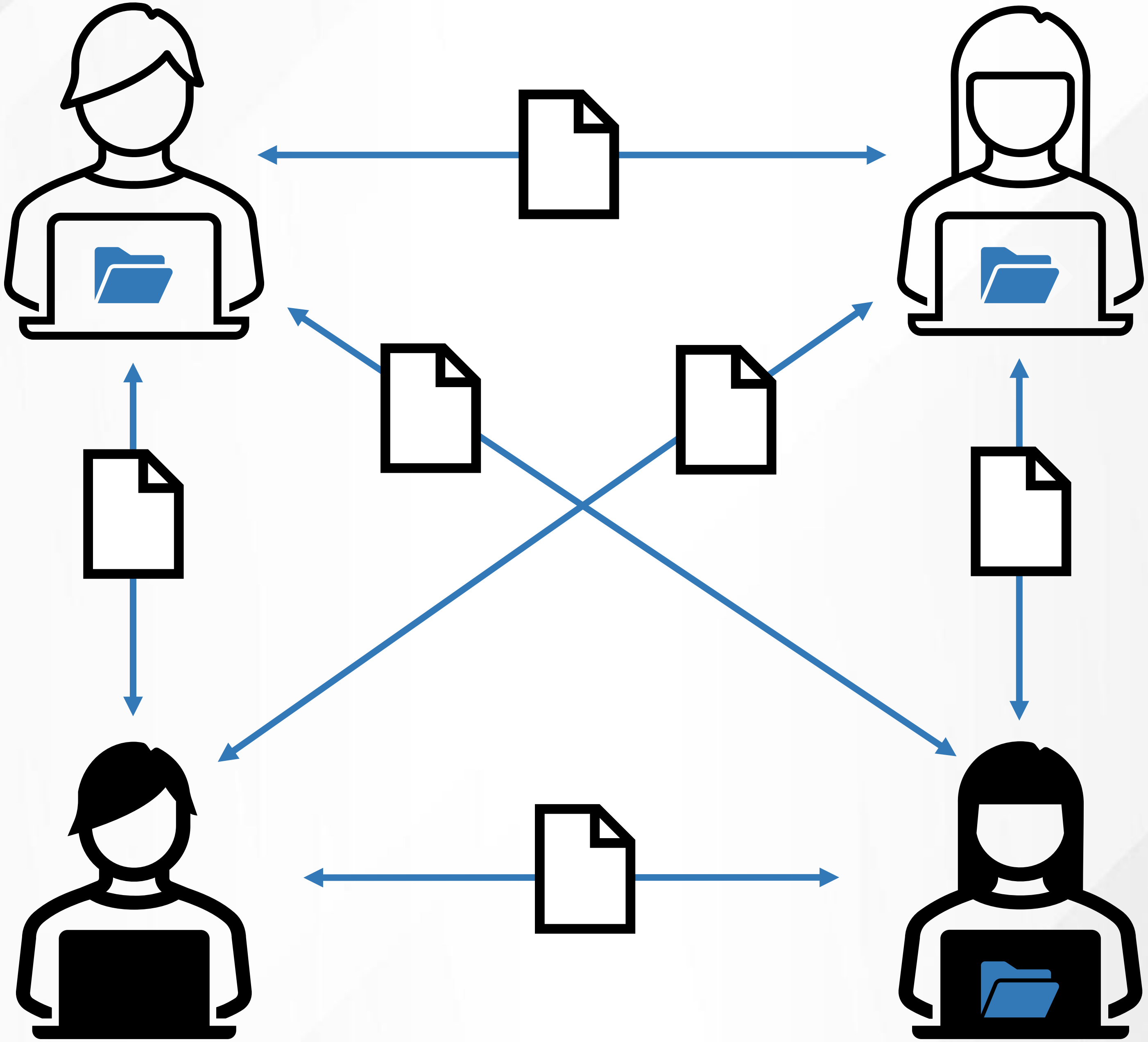
Story Time.

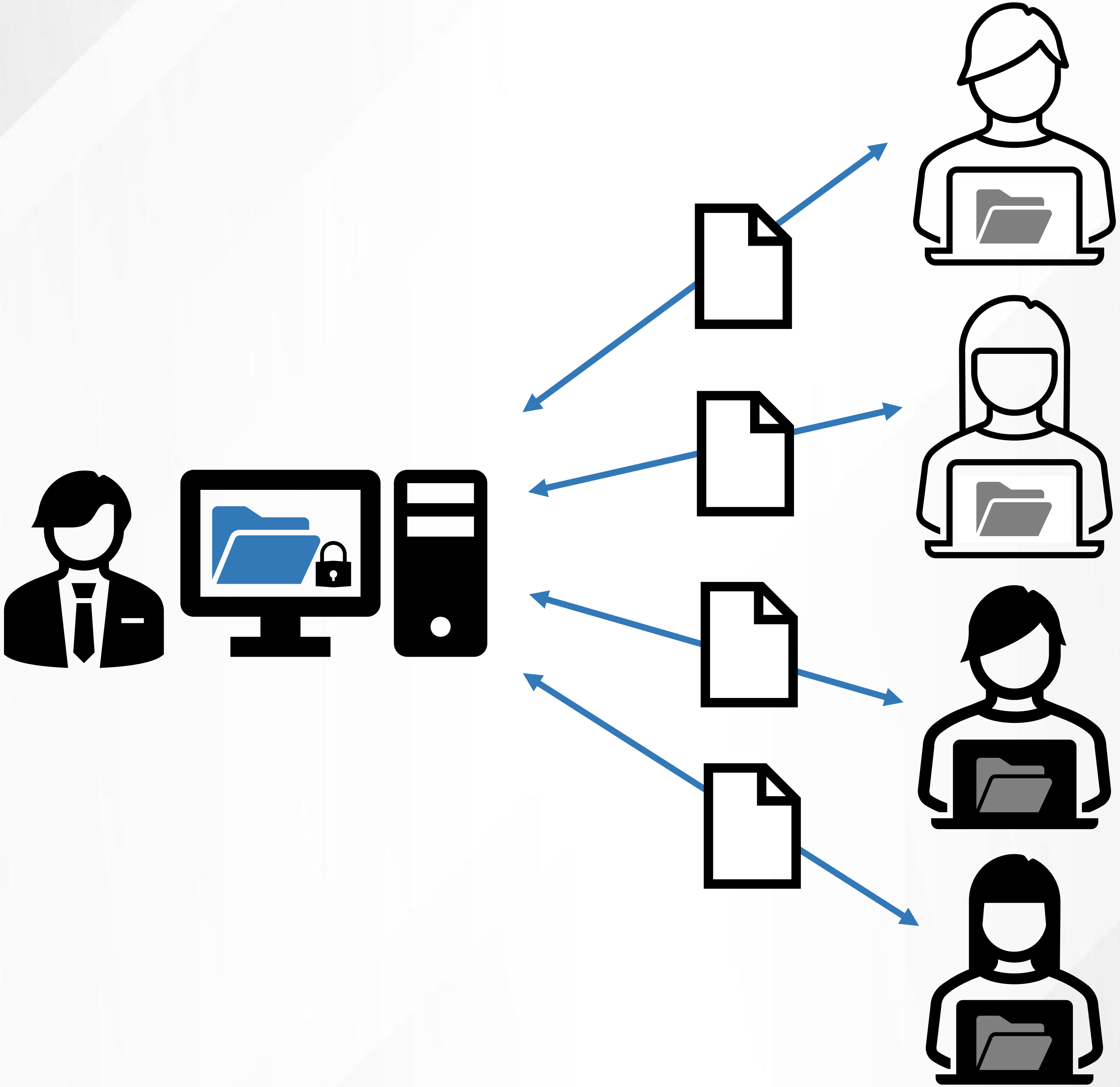
Legacy of Shares

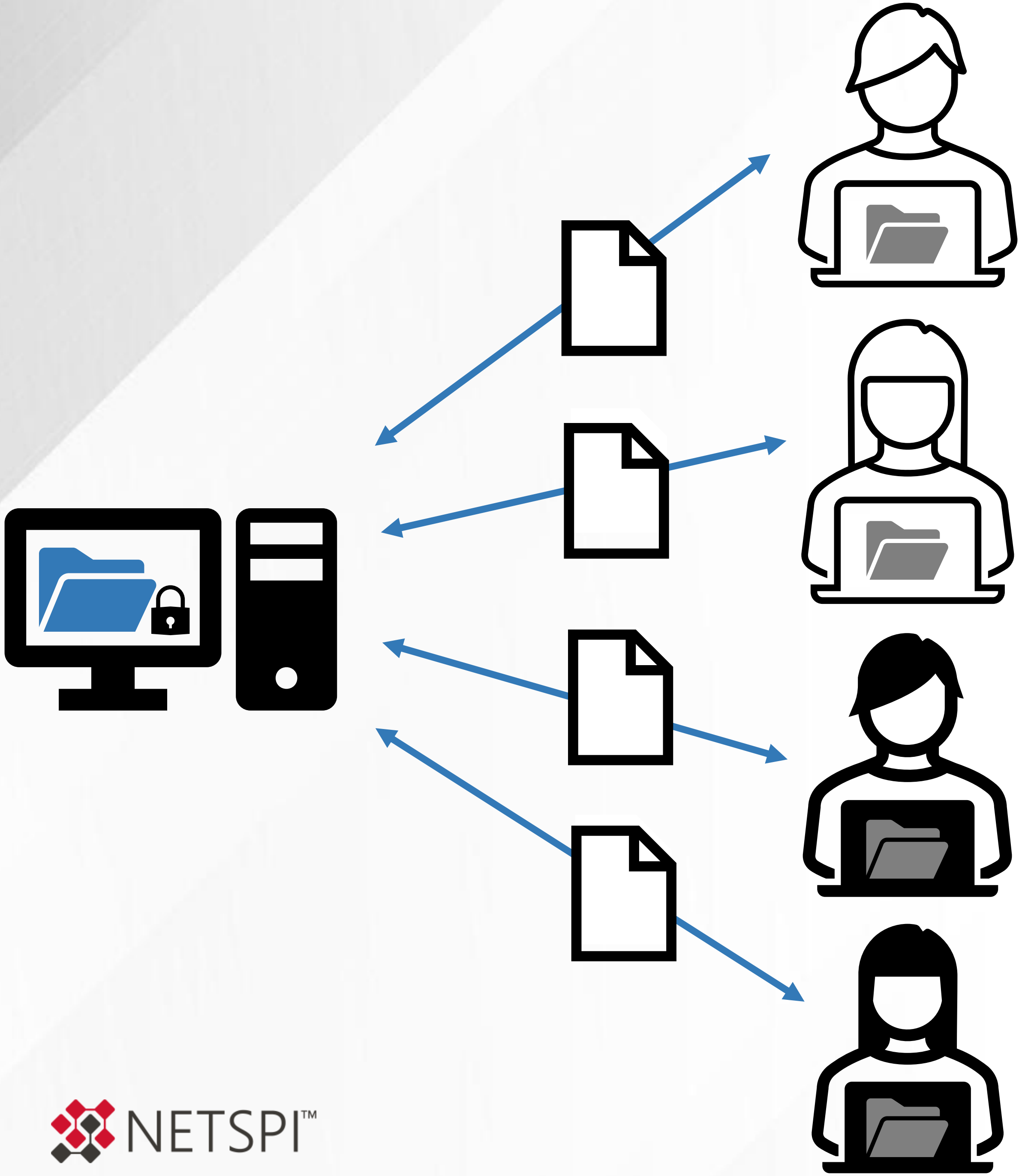


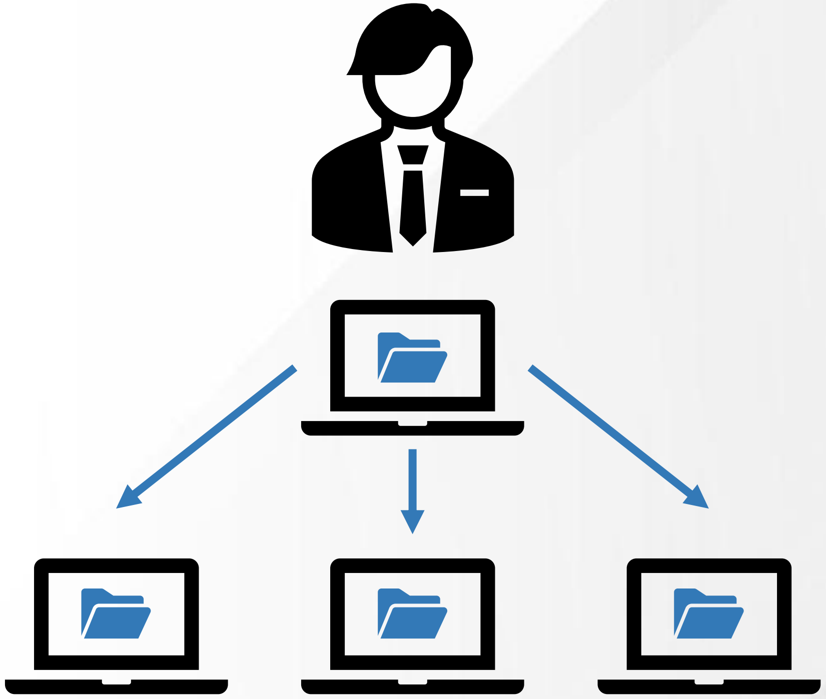


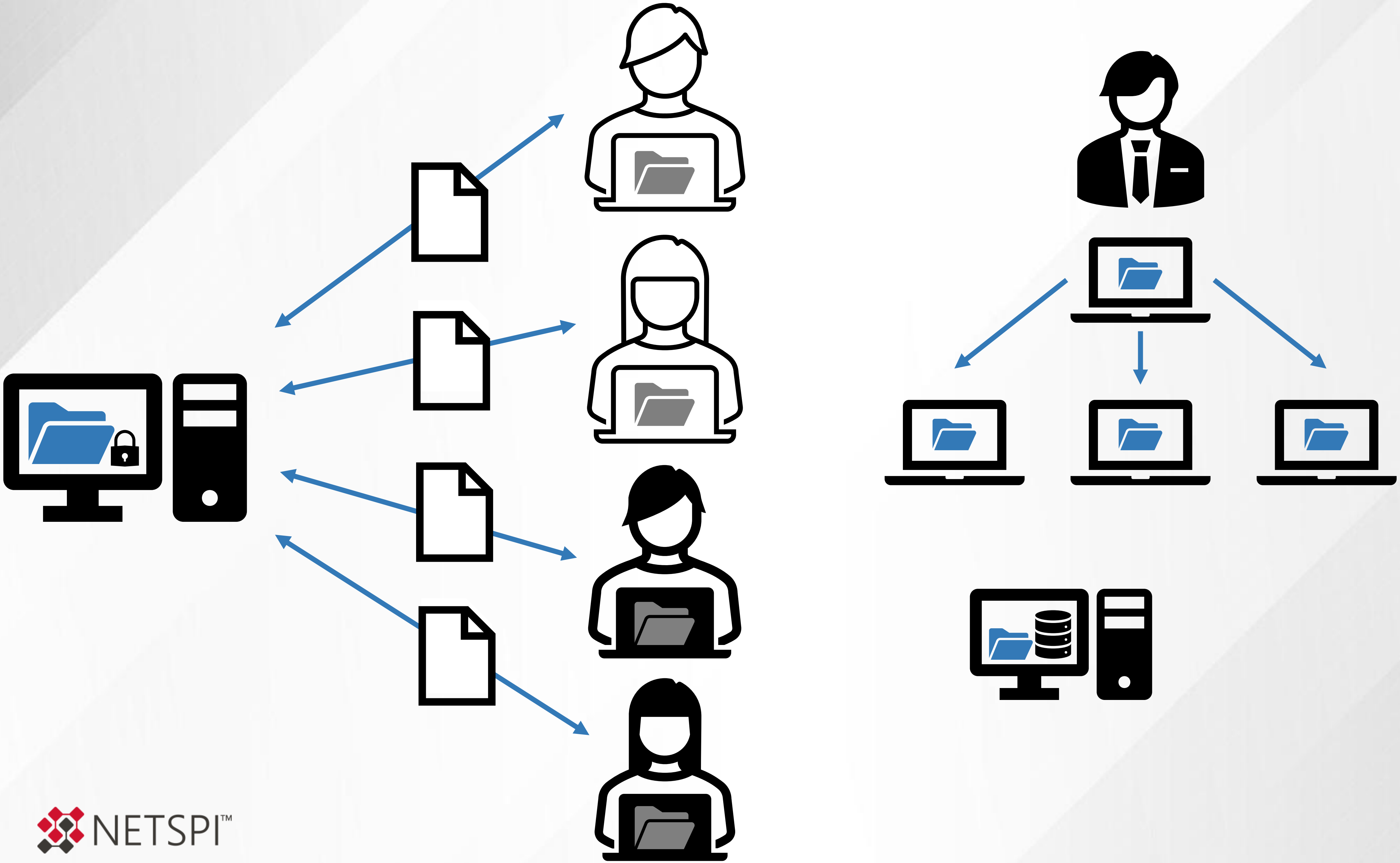


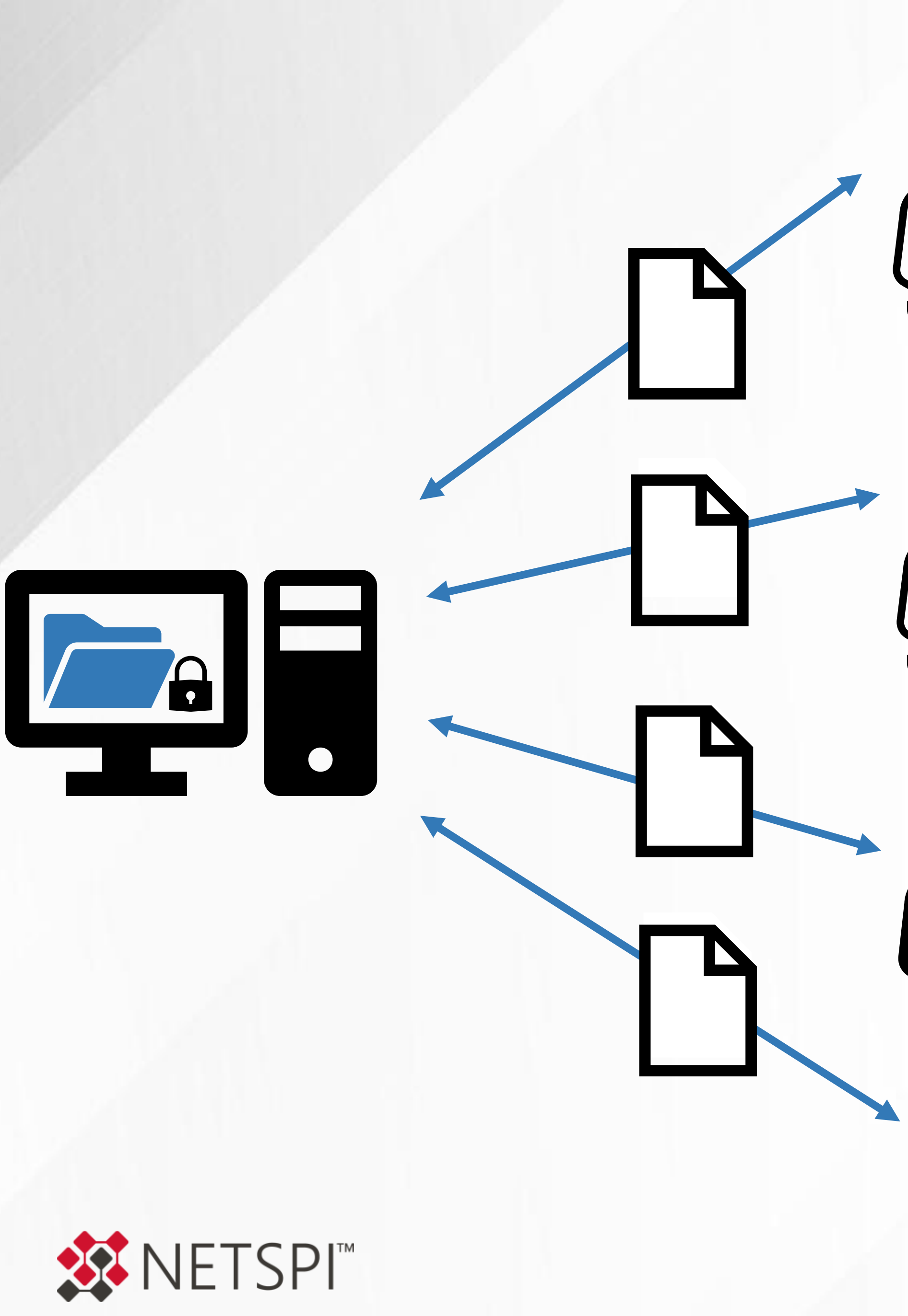


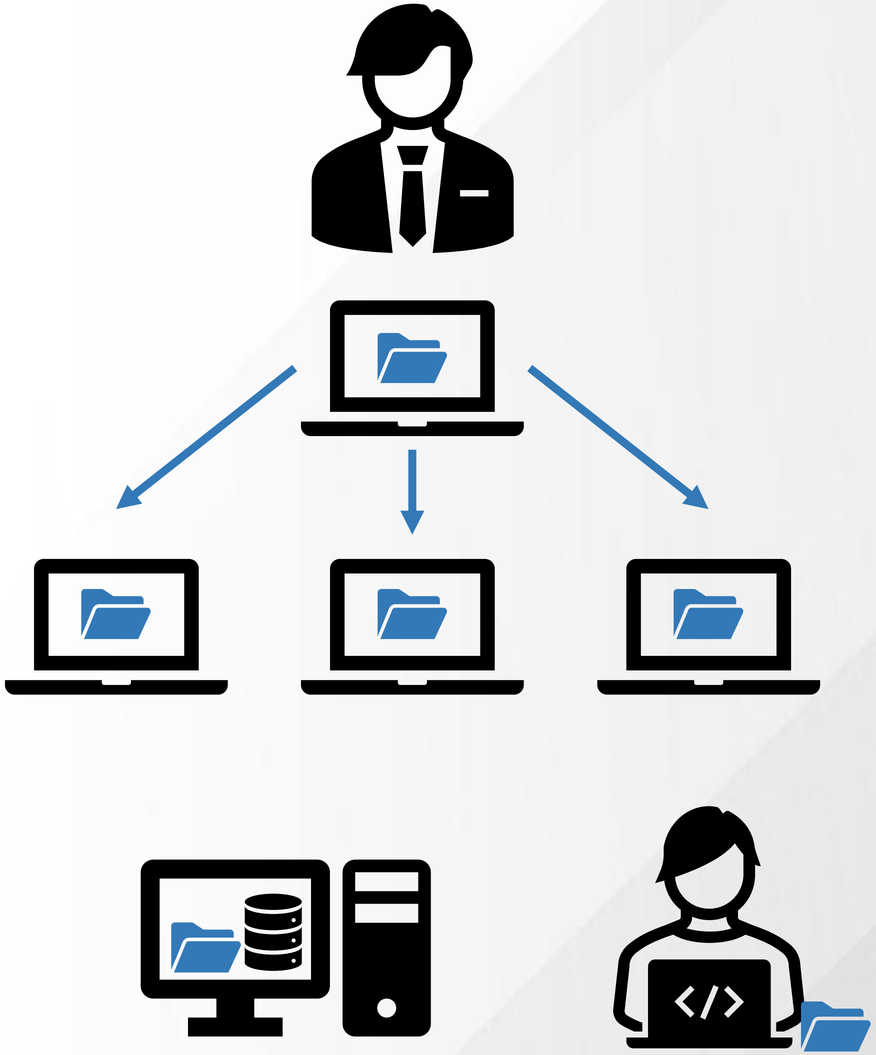


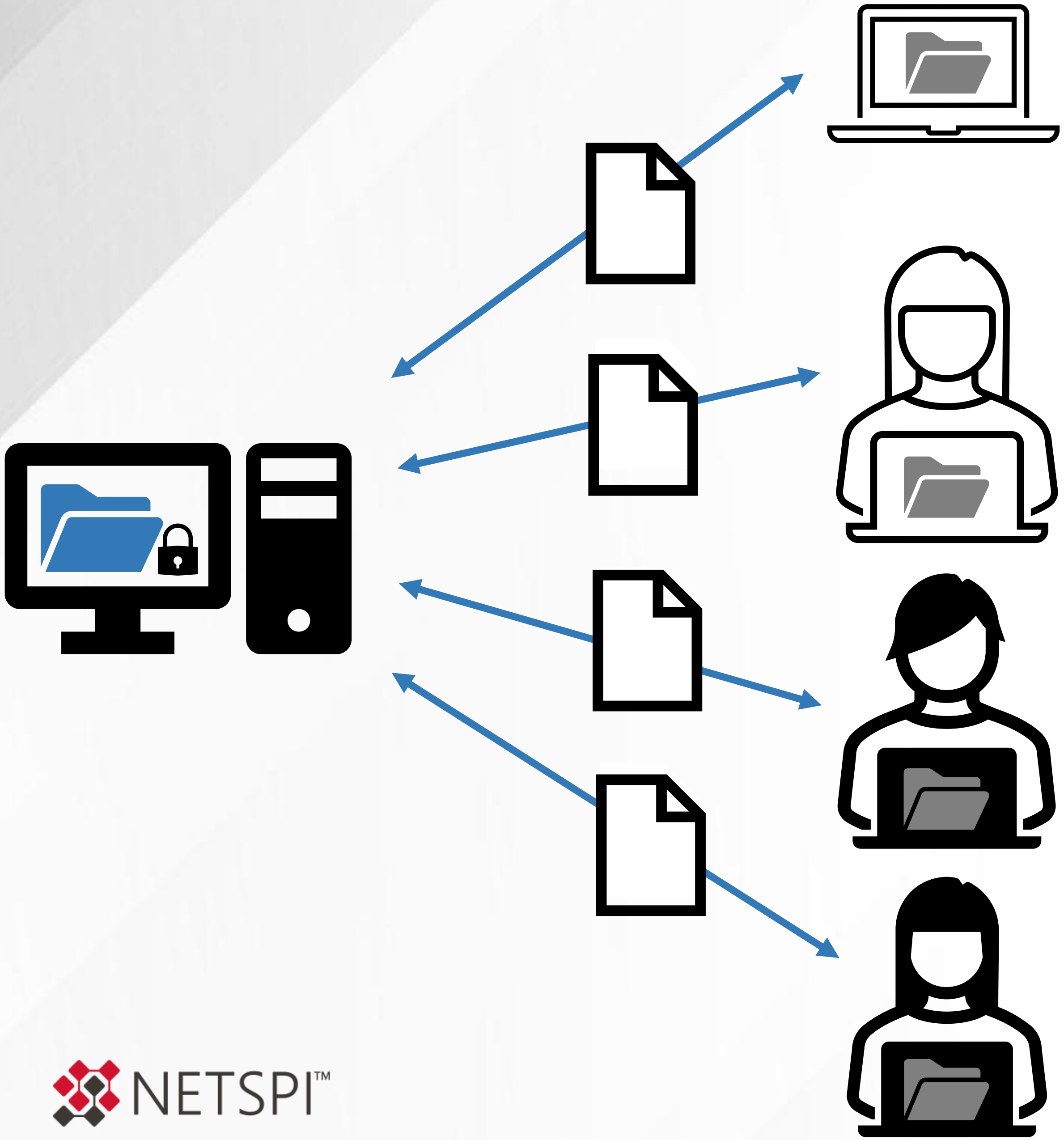


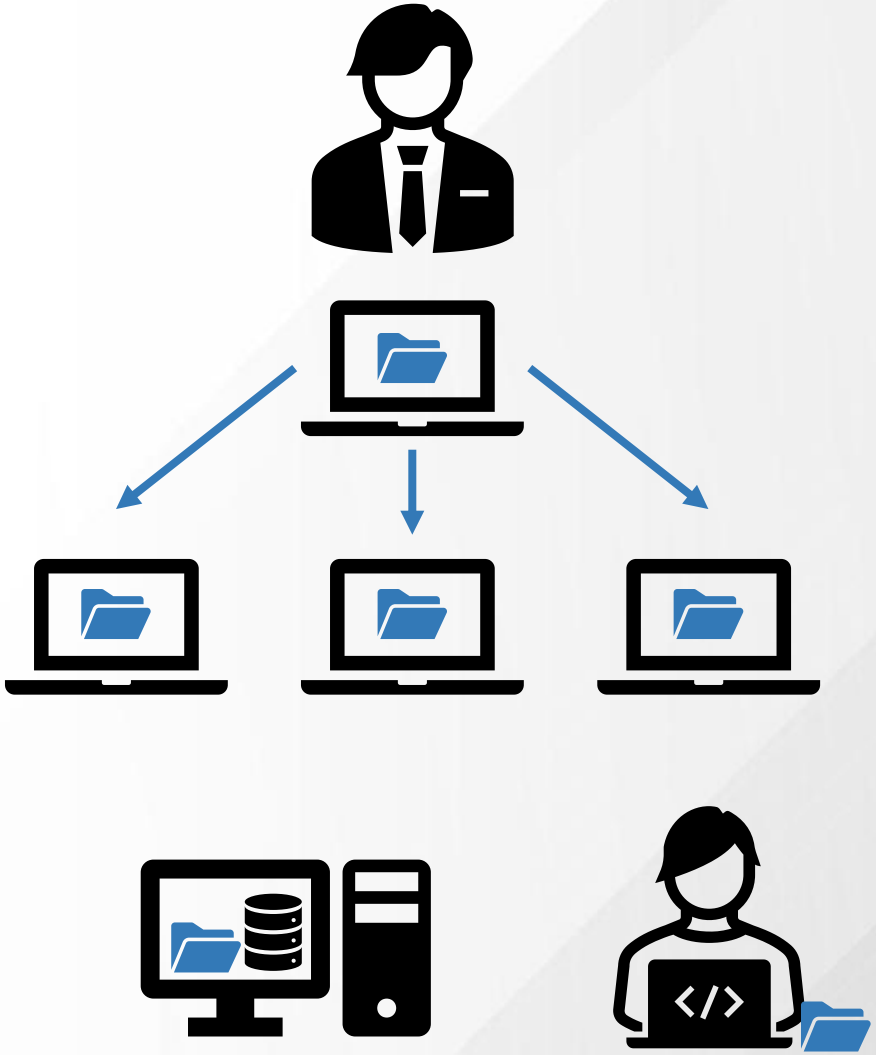


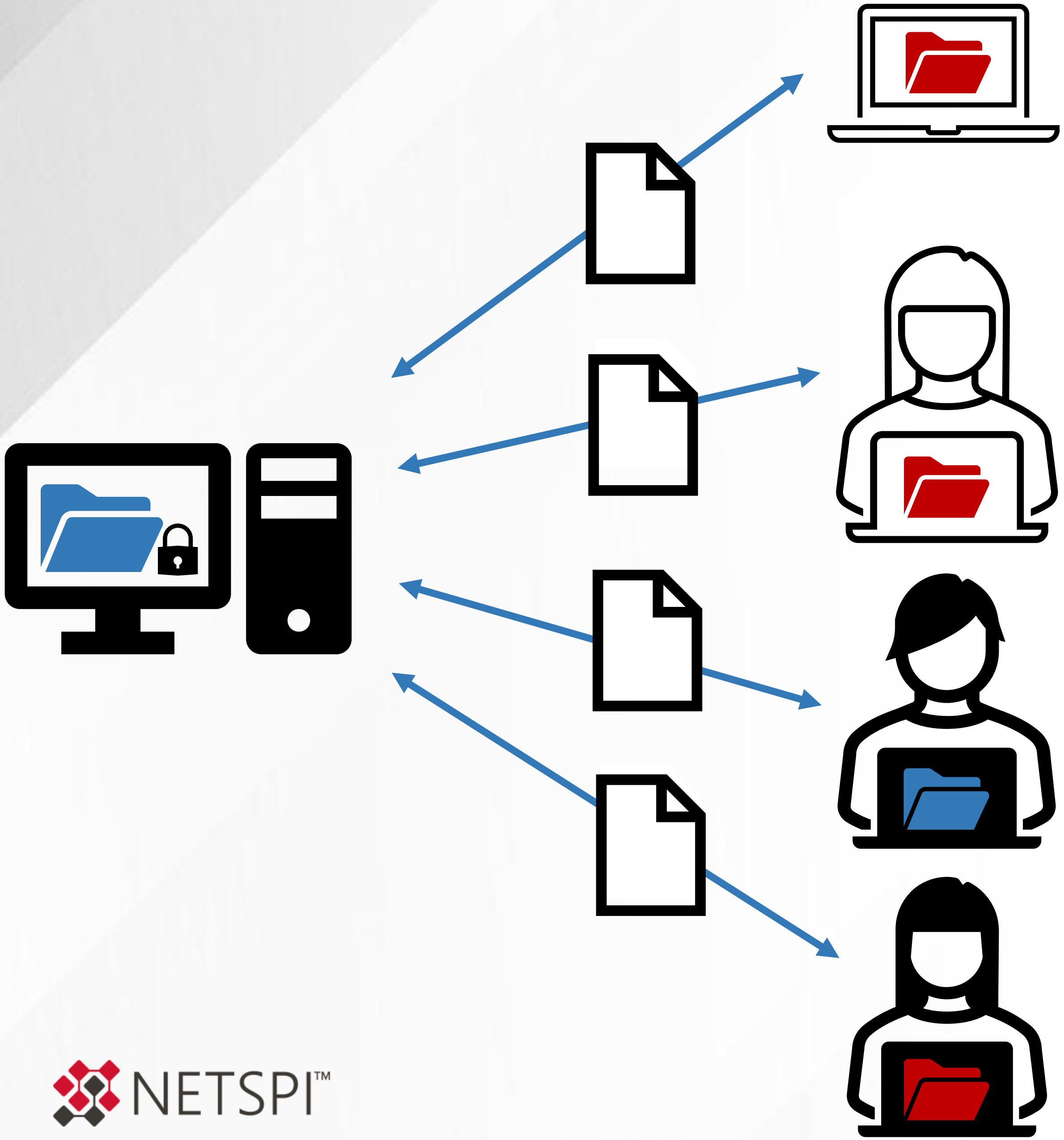


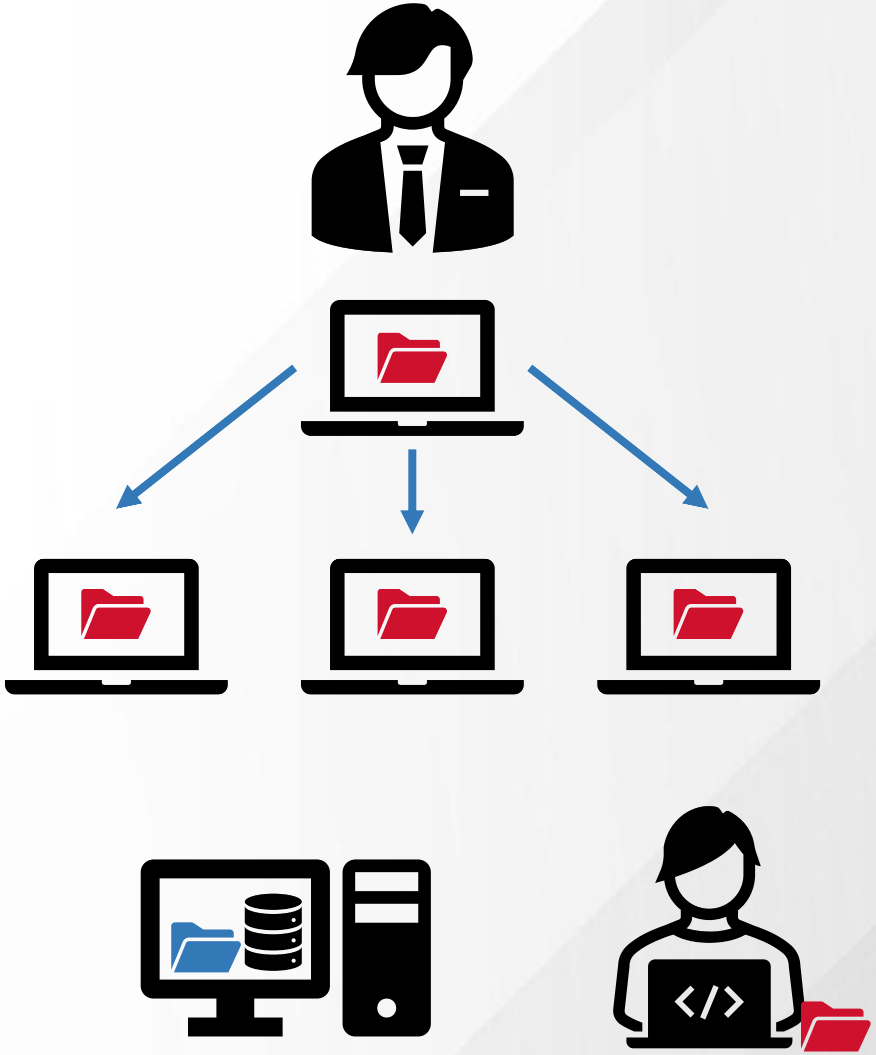




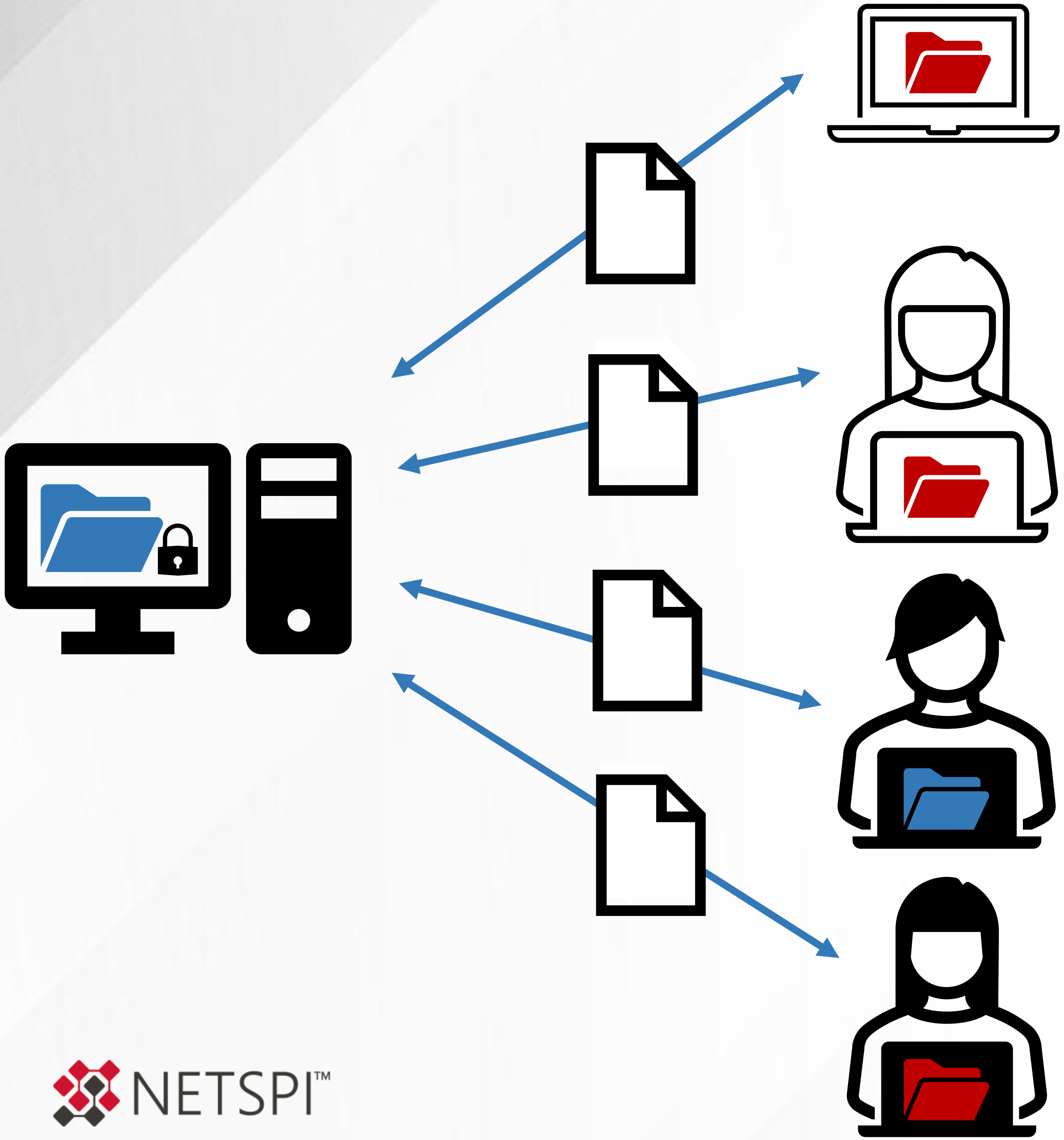


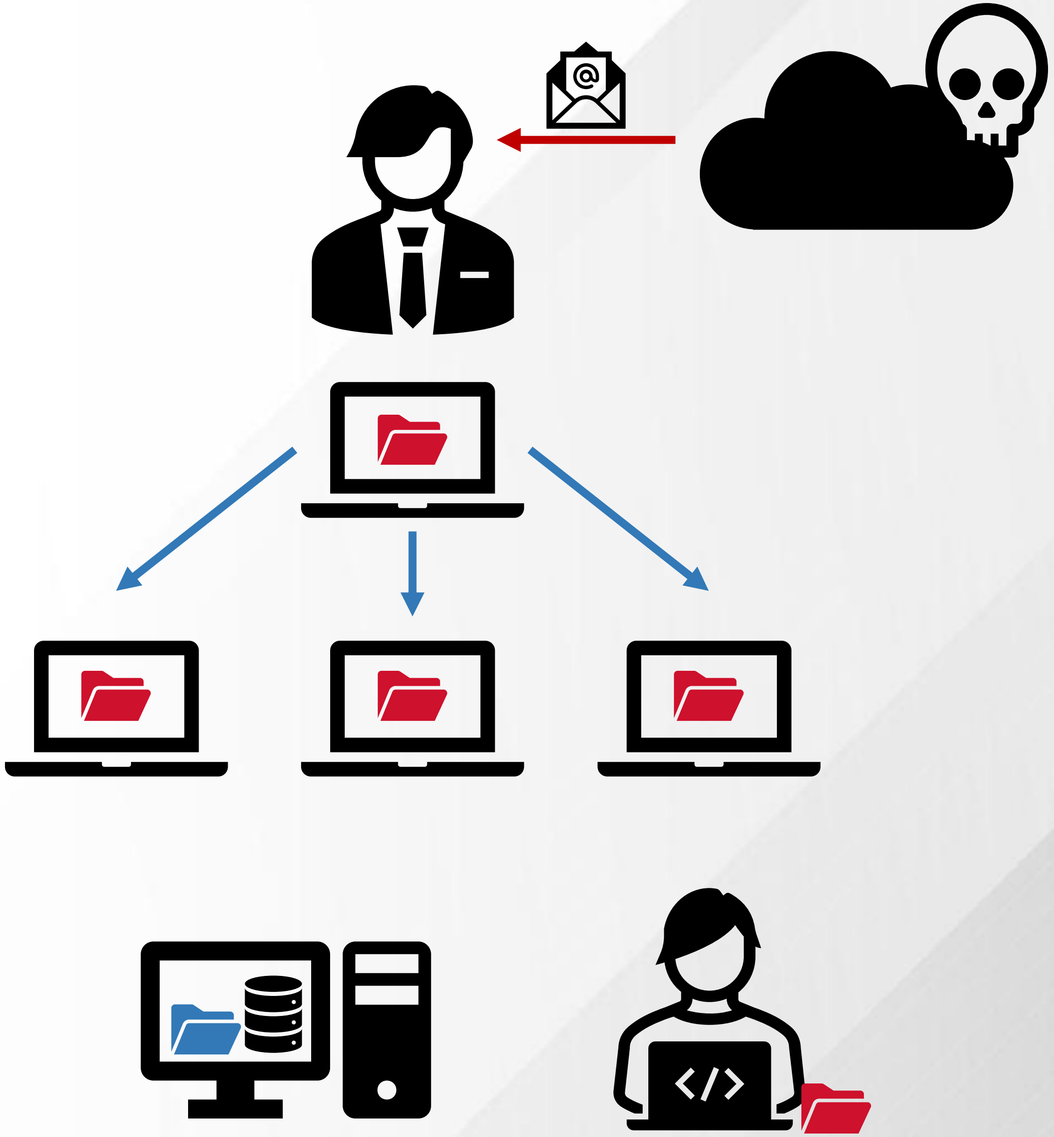


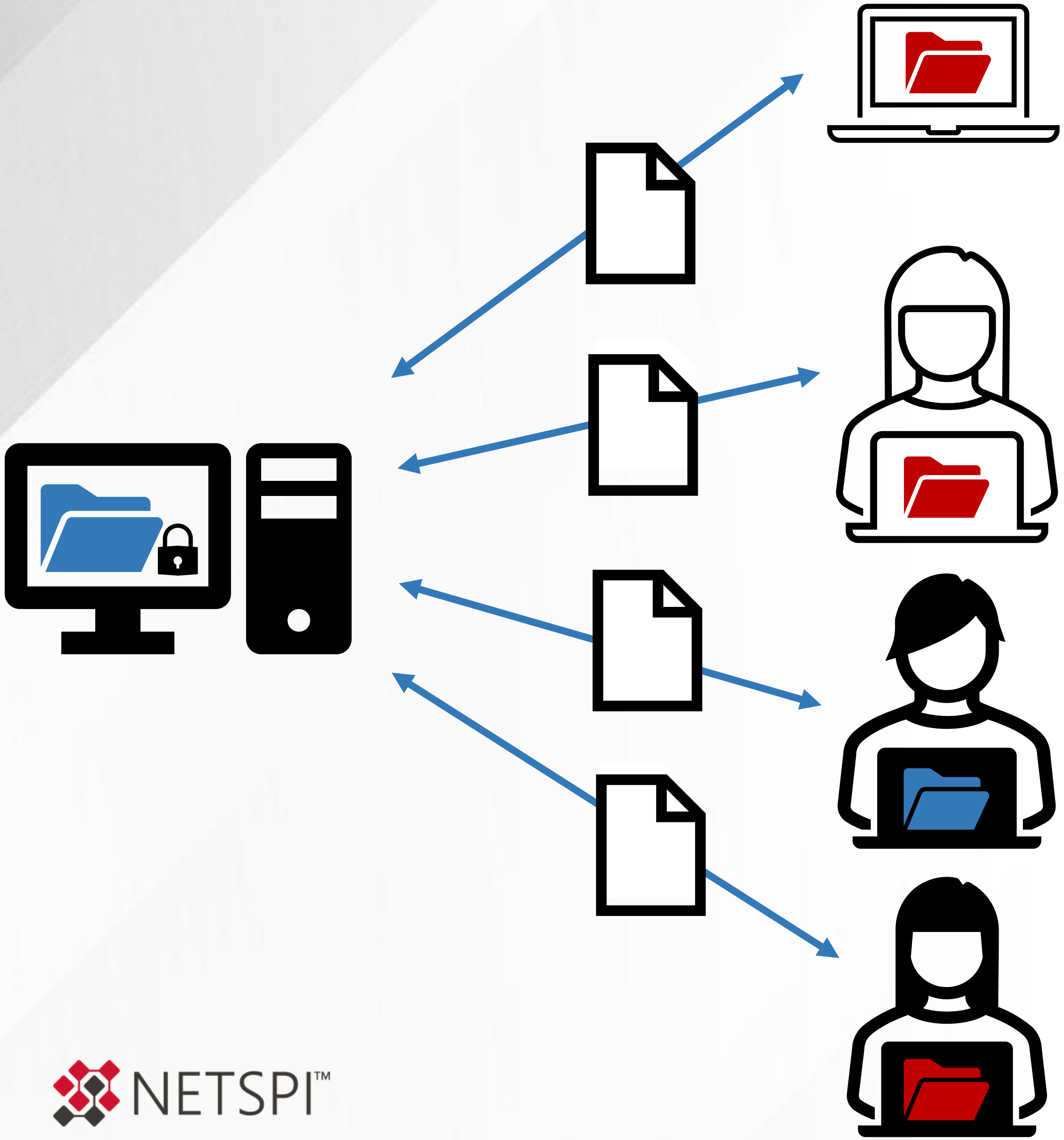


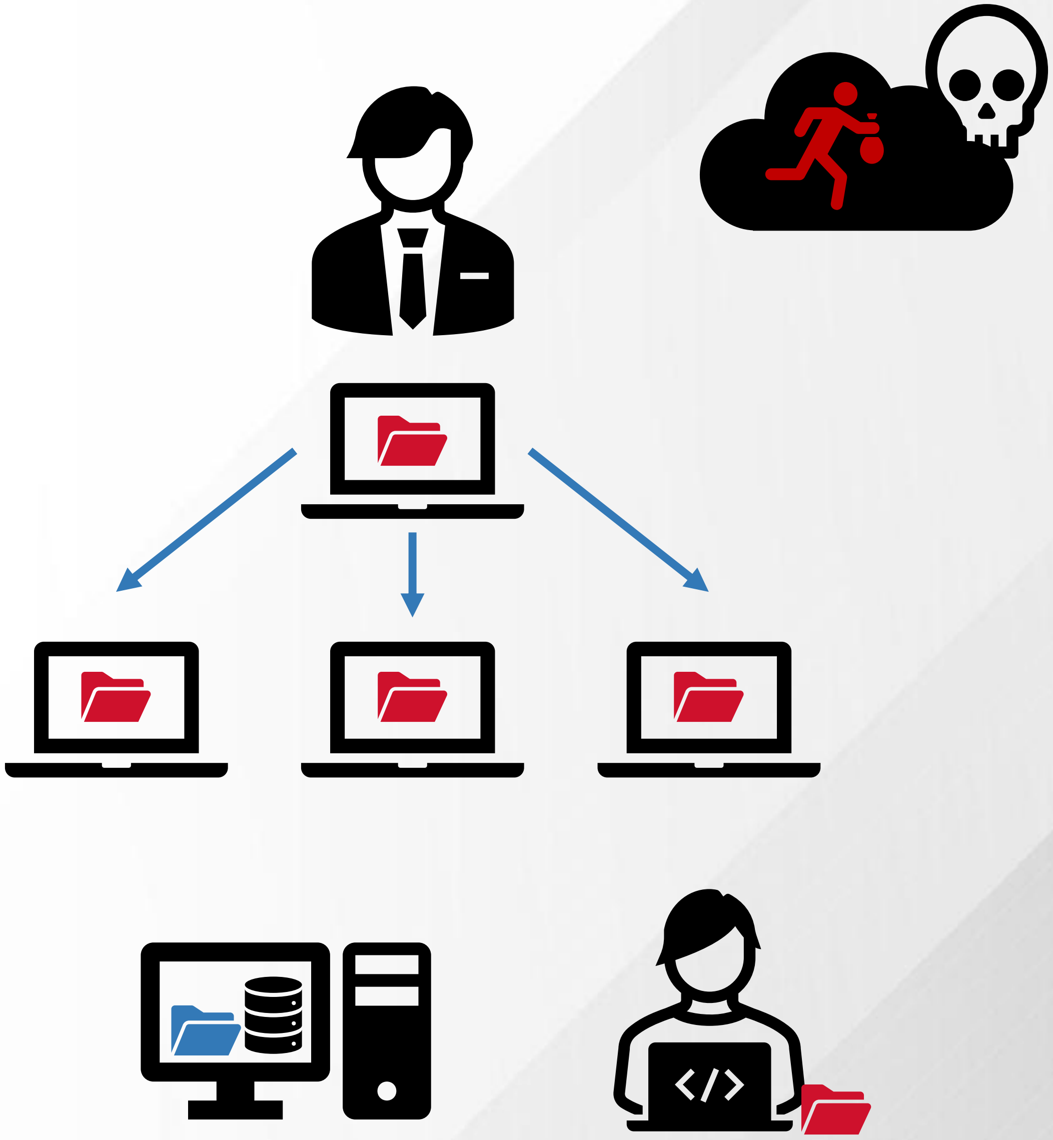


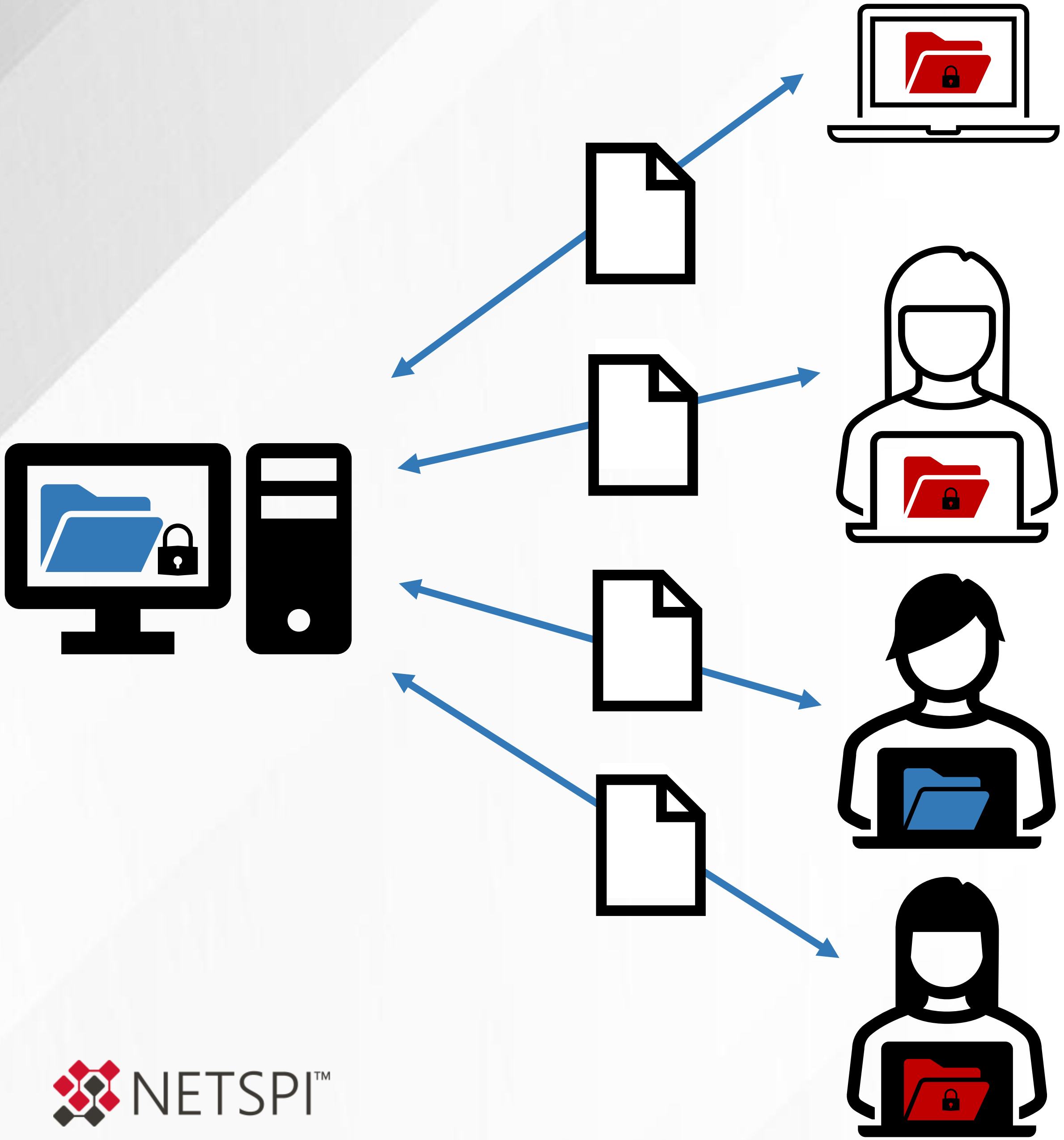
NETSPI™

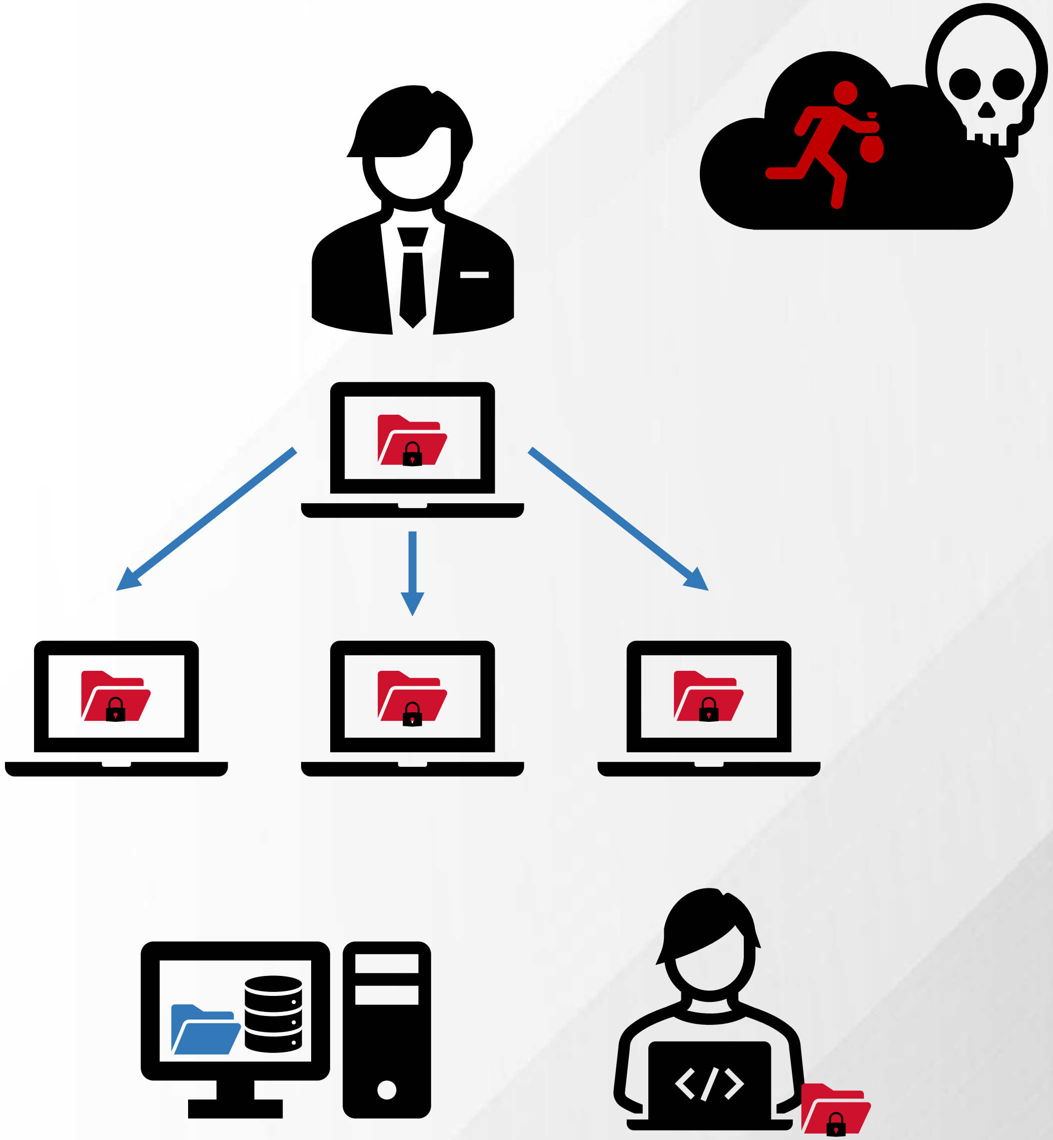




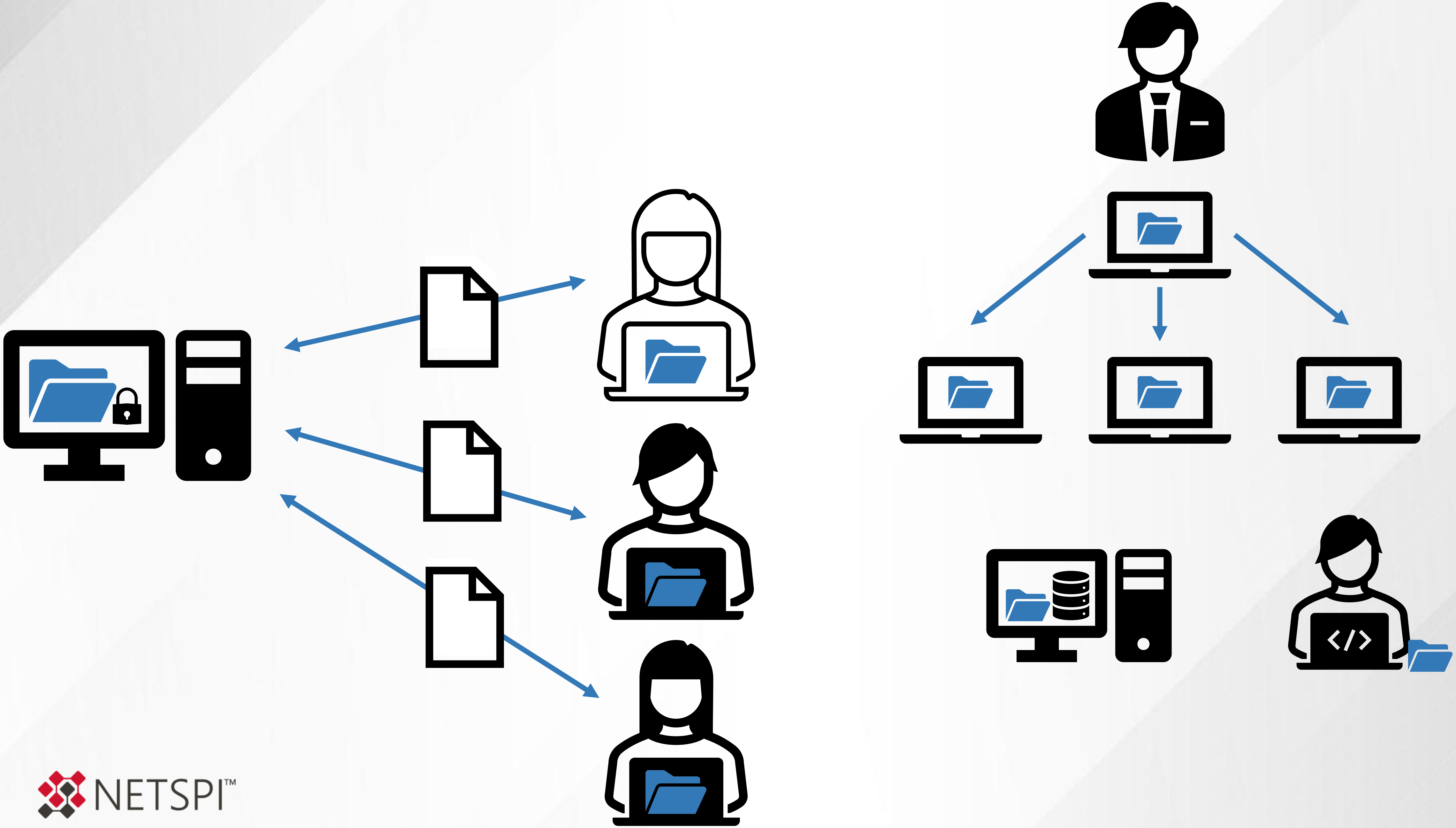


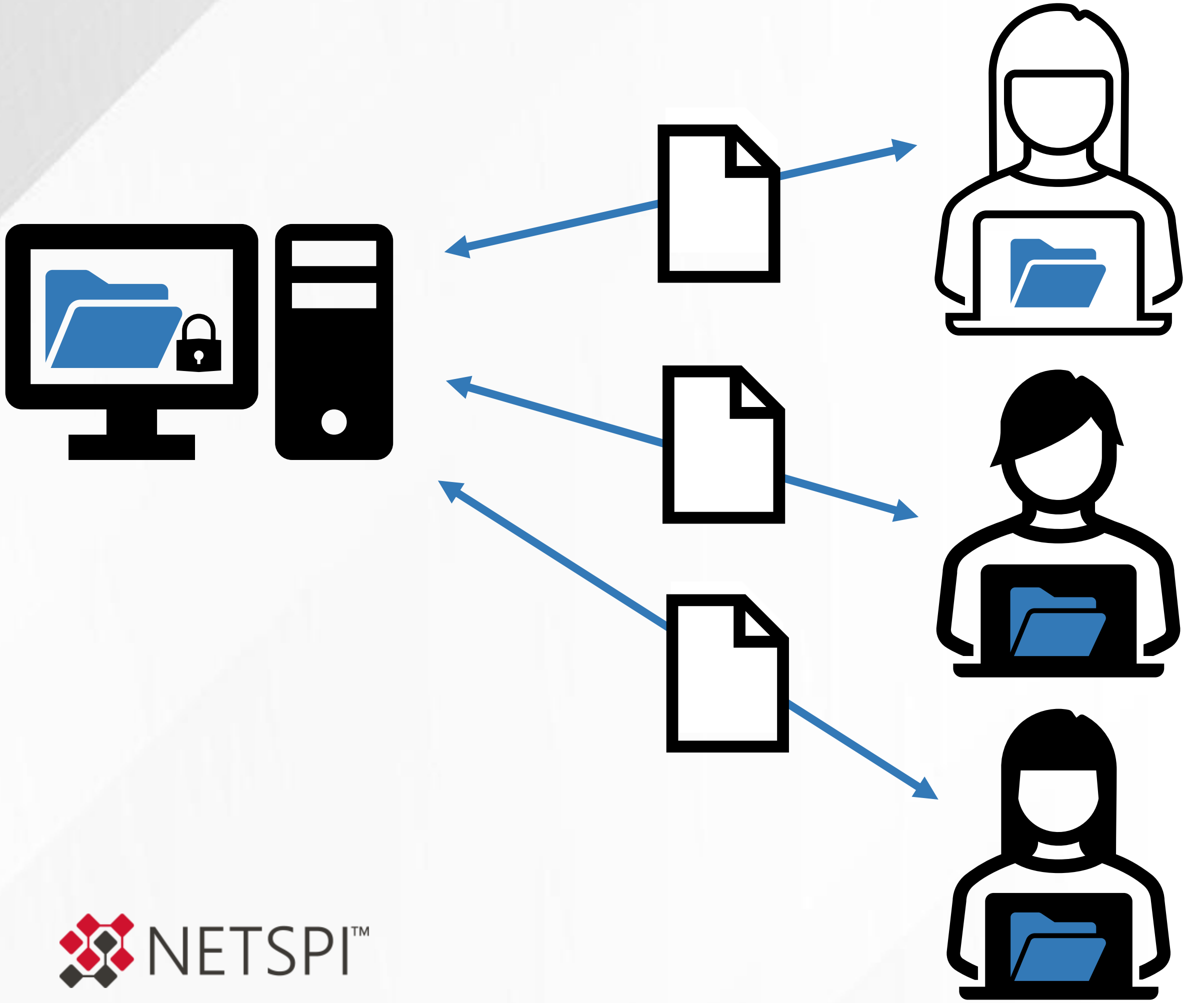


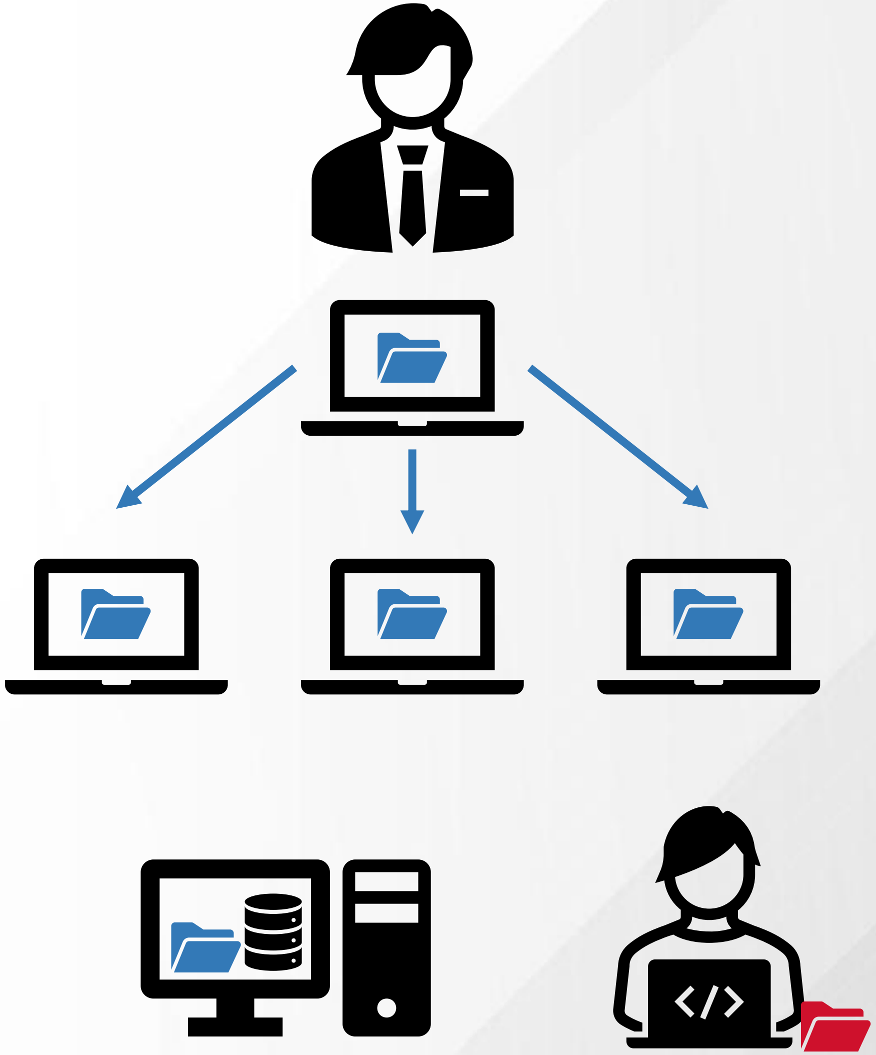


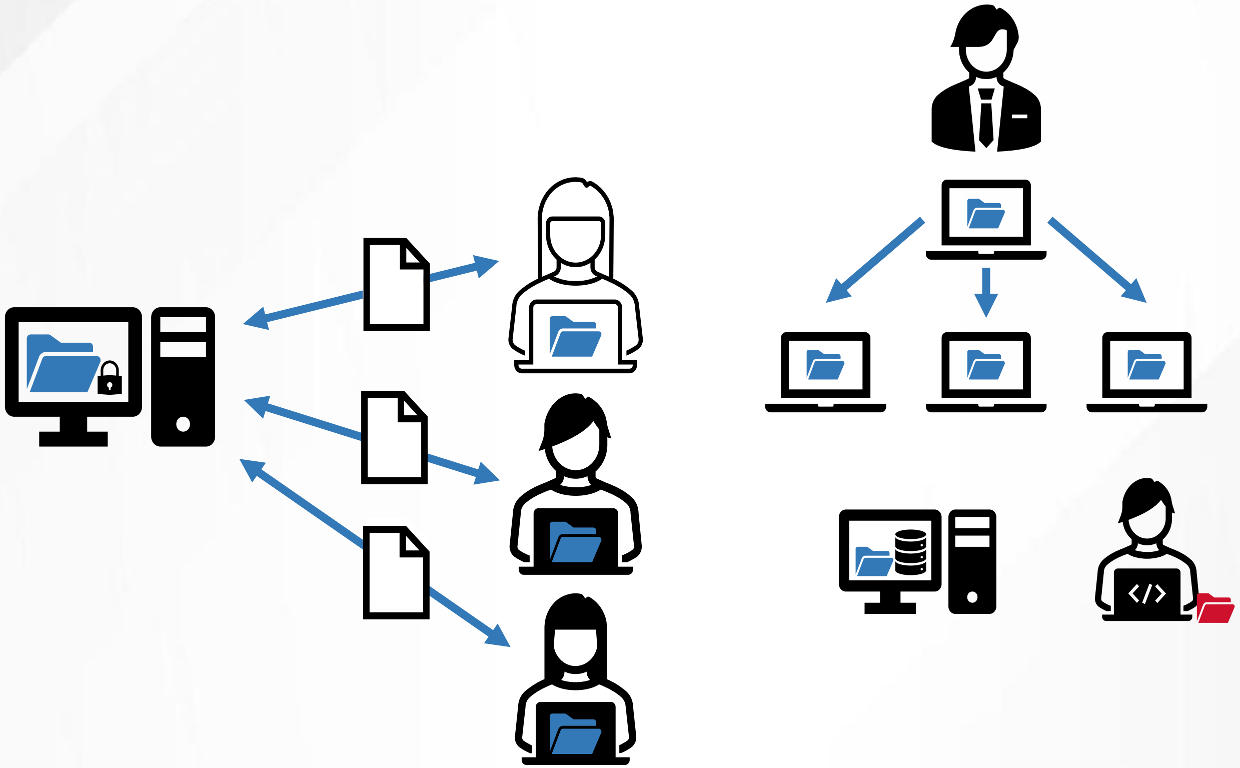


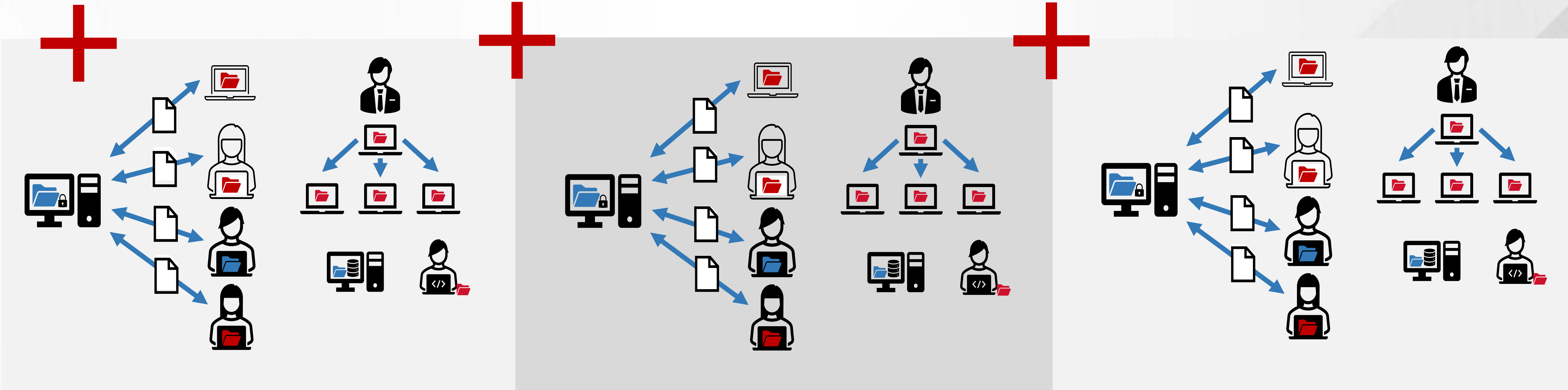
NETSPI™











This is a reality that a lot of businesses are trying to manage.

How can we identify the shares before the bad guys do?

How do we determine which shares represent actual risk?

How do we remediate a 100,000 shares configured with excessive privileges?

Into the Abyss: Evaluating Active Directory SMB Shares on Scale

What’s the Problem?

Why should I care about share permissions?

NETSPI™

What's the Problem?

- **Managing share inventory**

Managing shares on scale is hard!

Where are they?

System Inventory

Share Inventory

Who **owns** them?

What are the **Business Constraints?**

Change control

NETSPI™

What's the Problem?

- Managing share inventory
- Managing inherited permissions

Managing share permissions is hard!

Who needs access?

How do we provide that access?

When do we remove that access?

What are the **inherited Permissions?**

Remediation is hard on scale!

NETSPI™

What's the Problem?

- Managing share inventory
- Managing inherited permissions
- Vulnerability scanner gaps

Vulnerability scanners mis things!

A **full inventory** of shares

Shares available to **authenticated** users

High **risk** shares

Share permission **details**

Summary reports **with context**

Data that informs **remediation**

NETSPI™

What's the Problem?

- Managing share inventory
- Managing inherited permissions
- Vulnerability scanner gaps
- Shares are easy to exploit

Shares are easy to exploit!

SMB Shares are one of the **MOST** abused attacks surfaces

That require the **LEAST** amount of knowledge to attack

NETSPI™

What's the Problem?

- **Managing share inventory**
- **Managing inherited permissions**
- **Vulnerability scanner gaps**
- **Shares are easy to exploit**
- **Conclusion**

Conclusion

MOST vulnerability management programs overlook

high risk share exposure

NETSPI™

Into the Abyss: Evaluating Active Directory SMB Shares on Scale

Share Permissions Primer

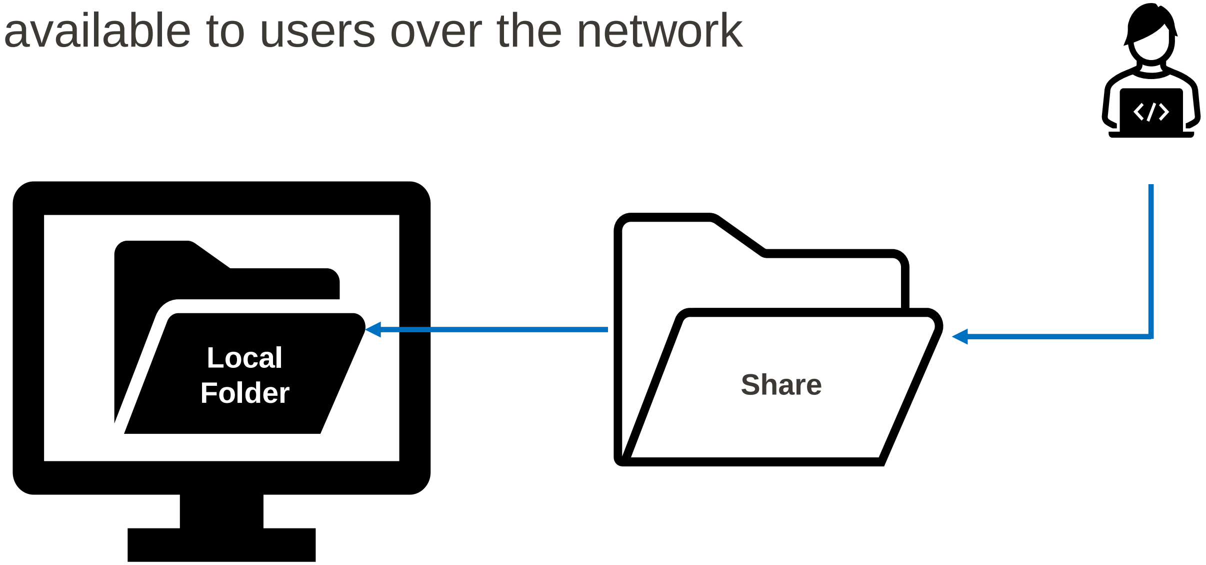
How do they work and where do things go wrong?

Share Permissions

- What's a share?

What's a share?

A share is basically a local folder made available to users over the network



Share Permissions

- What’s a share?
- Access control

Access Control

Access to shared folders are controlled through NTFS and share permissions

NTFS

- Used to control access to the NTFS file system
- Can affect local and network users
- More granular than share permissions

Share

- Used to control access to shared files and folders
- Do not apply to local users
- Less granular permissions

NETSPI™

Share Permissions

- What's a share?
- Access control

Access Control

Access to shared folders are controlled through NTFS and share permissions

Most restrictive permissions win!

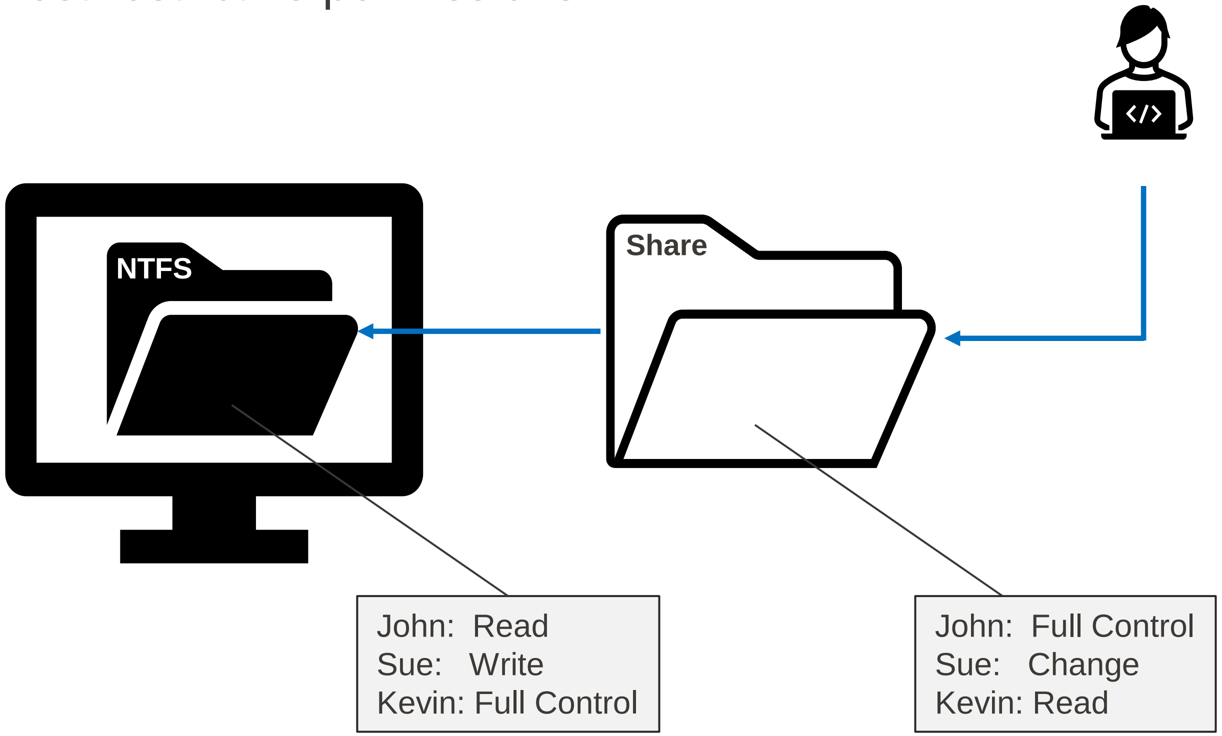
NETSPI™

Share Permissions

- **What's a share?**
- **Access control**

Access Control

Most restrictive permissions win!



John: Read
Sue: Write
Kevin: Full Control

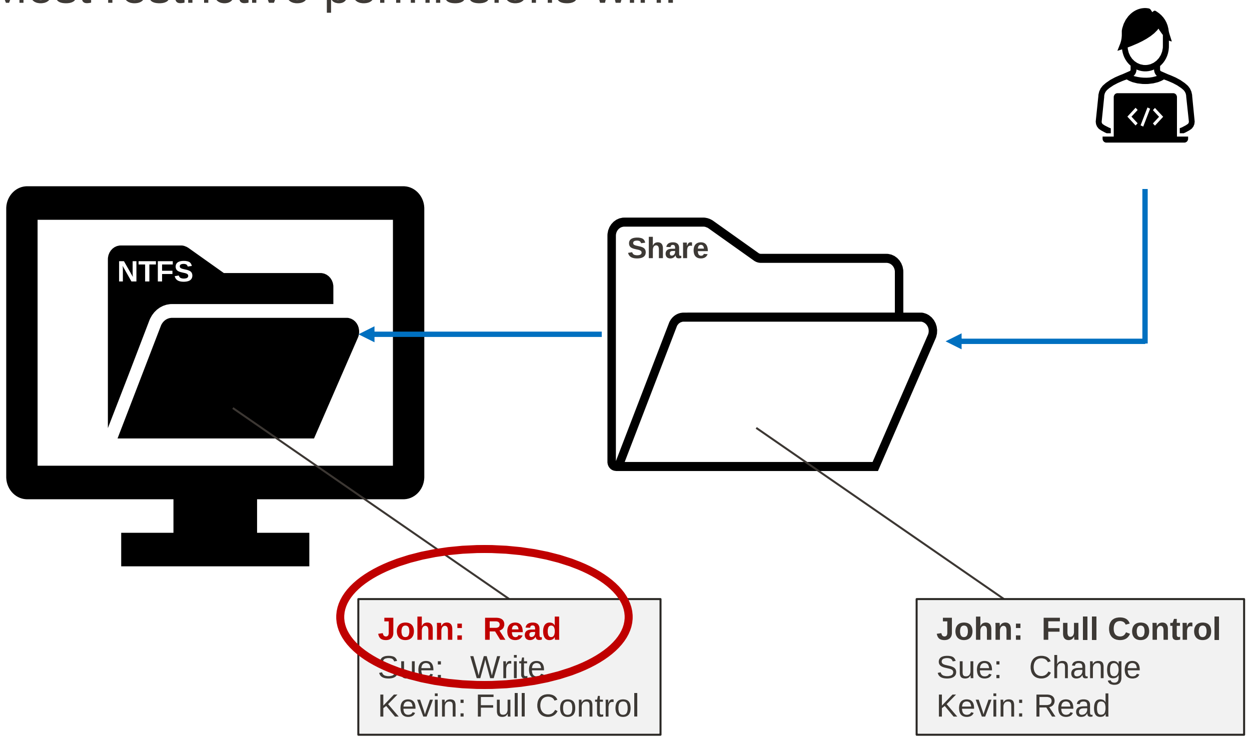
John: Full Control
Sue: Change
Kevin: Read

Share Permissions

- What's a share?
- Access control

Access Control

Most restrictive permissions win!



John: Read
Sue: Write
Kevin: Full Control

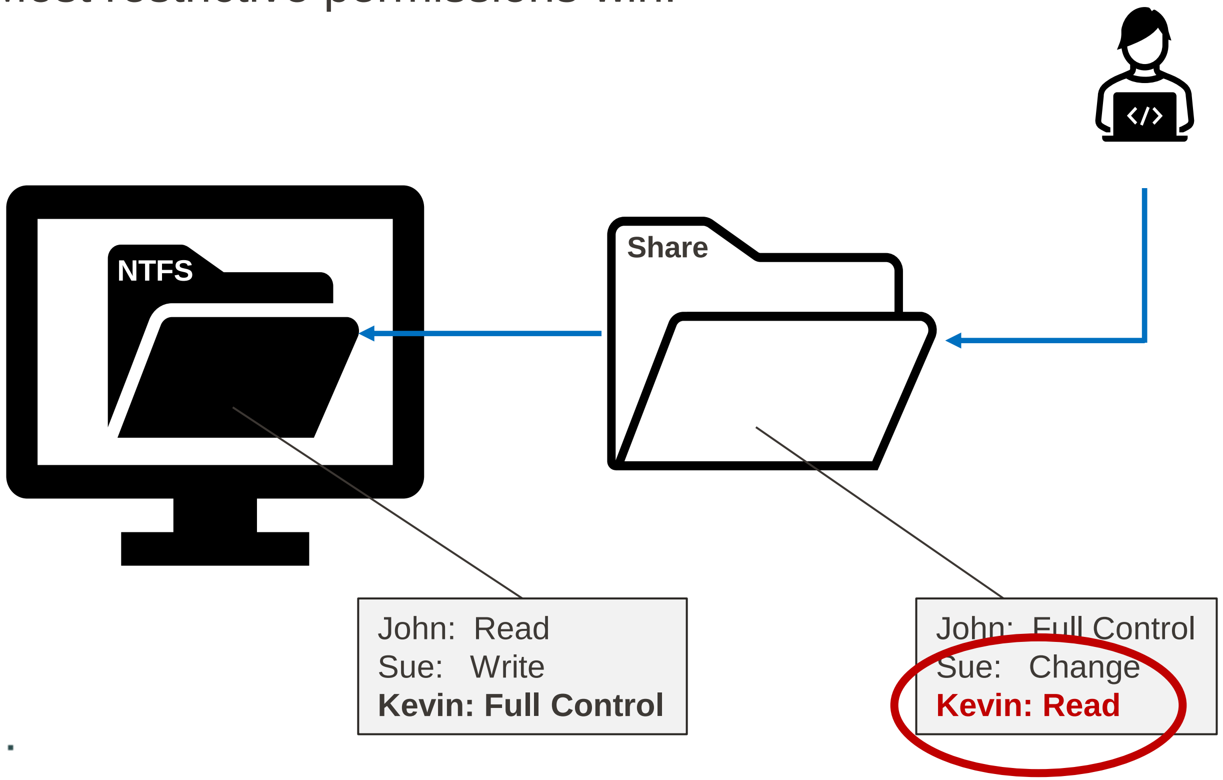
John: Full Control
Sue: Change
Kevin: Read

Share Permissions

- What's a share?
- Access control

Access Control

Most restrictive permissions win!



John: Read
Sue: Write
Kevin: Full Control

John: Full Control
Sue: Change
Kevin: Read

unfortunately, things aren’t quite that simple

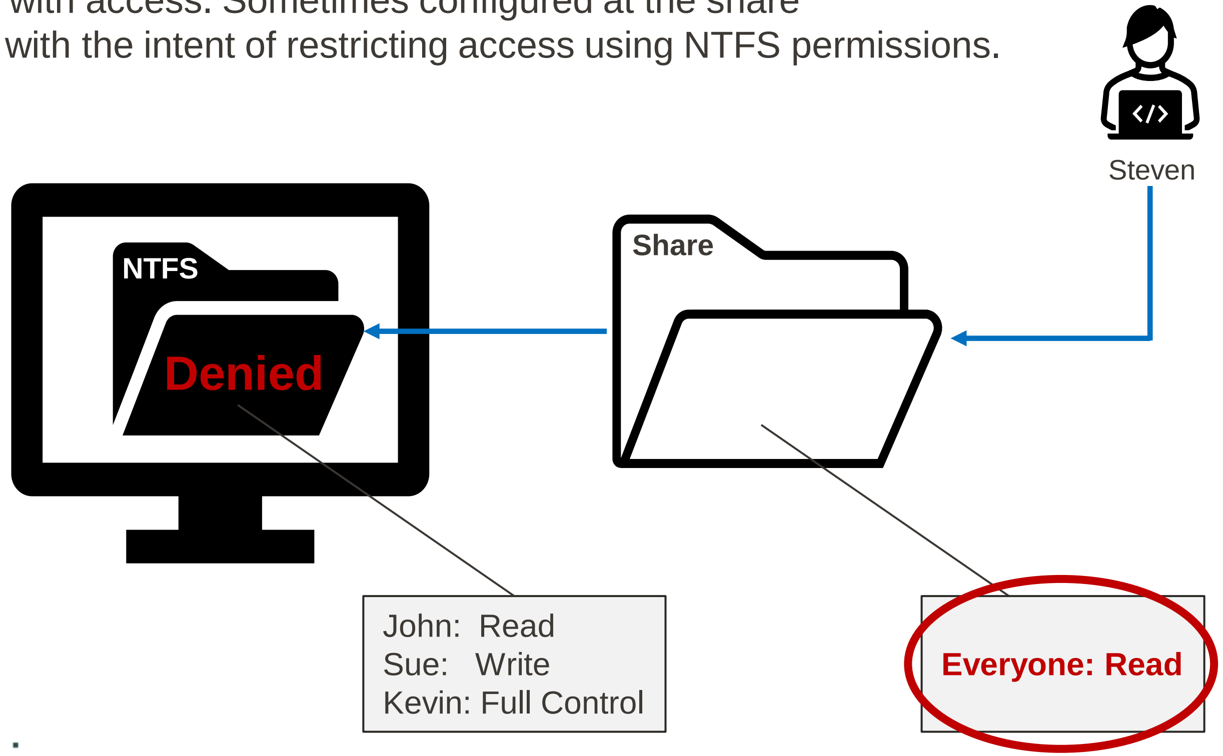
Share Permissions

- What’s a share?
- Access control
- NTFS vs share priority

- Everyone

Everyone Group

Can provide unauthenticated and authenticated users with access. Sometimes configured at the share level, with the intent of restricting access using NTFS permissions.



John: Read
Sue: Write
Kevin: Full Control

Everyone: Read

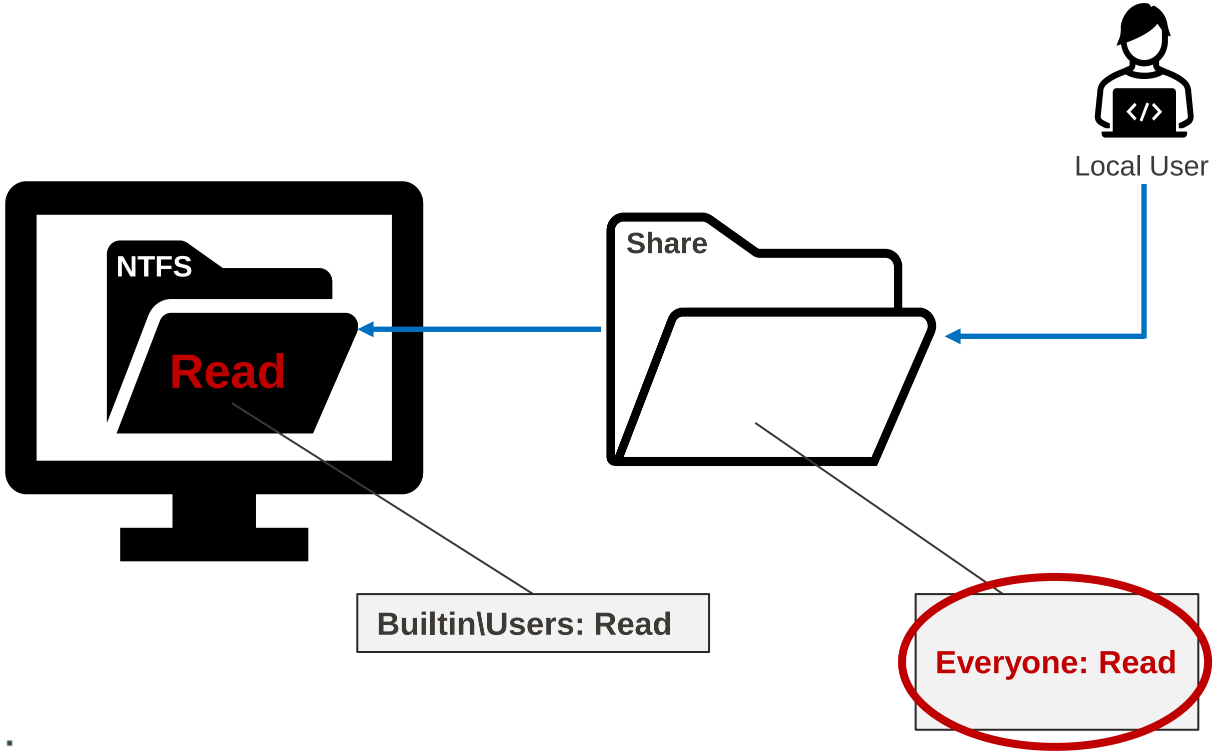
Share Permissions

- What's a share?
- Access control
- NTFS vs share priority

- Everyone
- Builtin\Users

Builtin\Users

Should only provide the local users with access.



Share Permissions

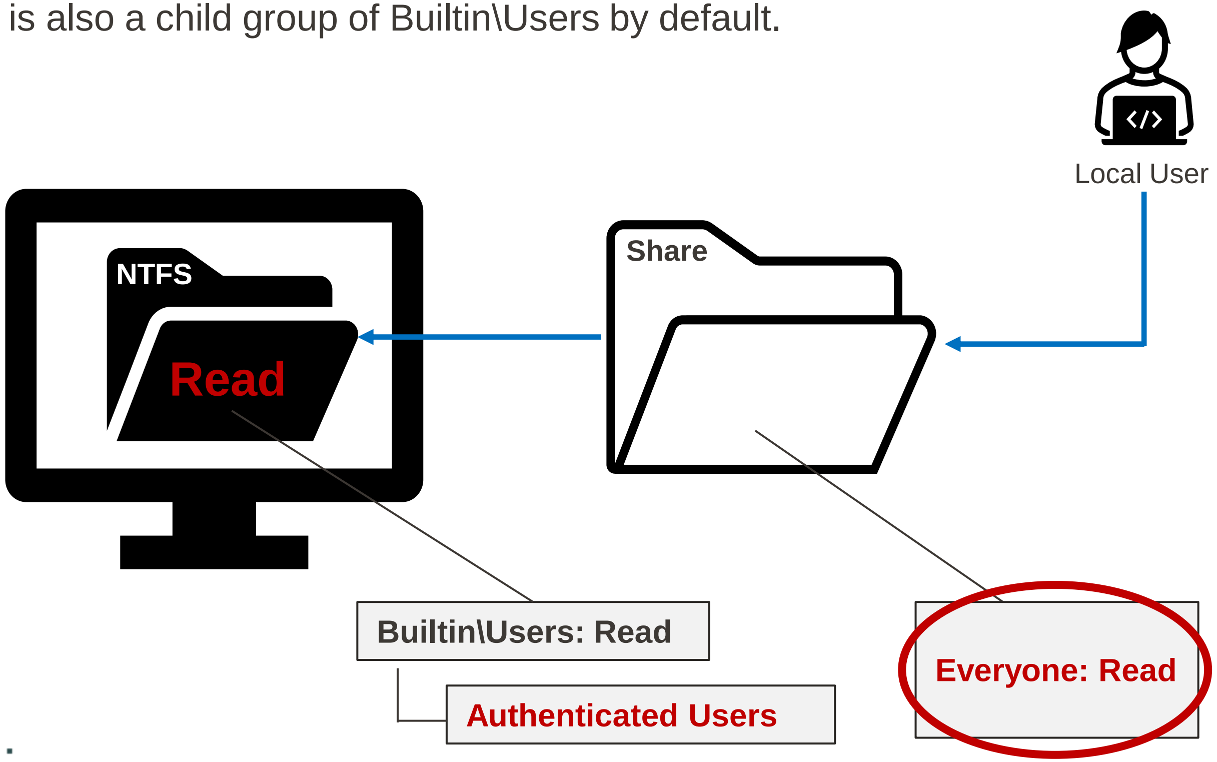
- What's a share?
- Access control
- NTFS vs share priority

- Everyone
- Builtin\Users
- Authenticated Users

Authenticated Users

Limited to local user accounts when NOT on an AD domain.

This is also a child group of Builtin\Users by default.



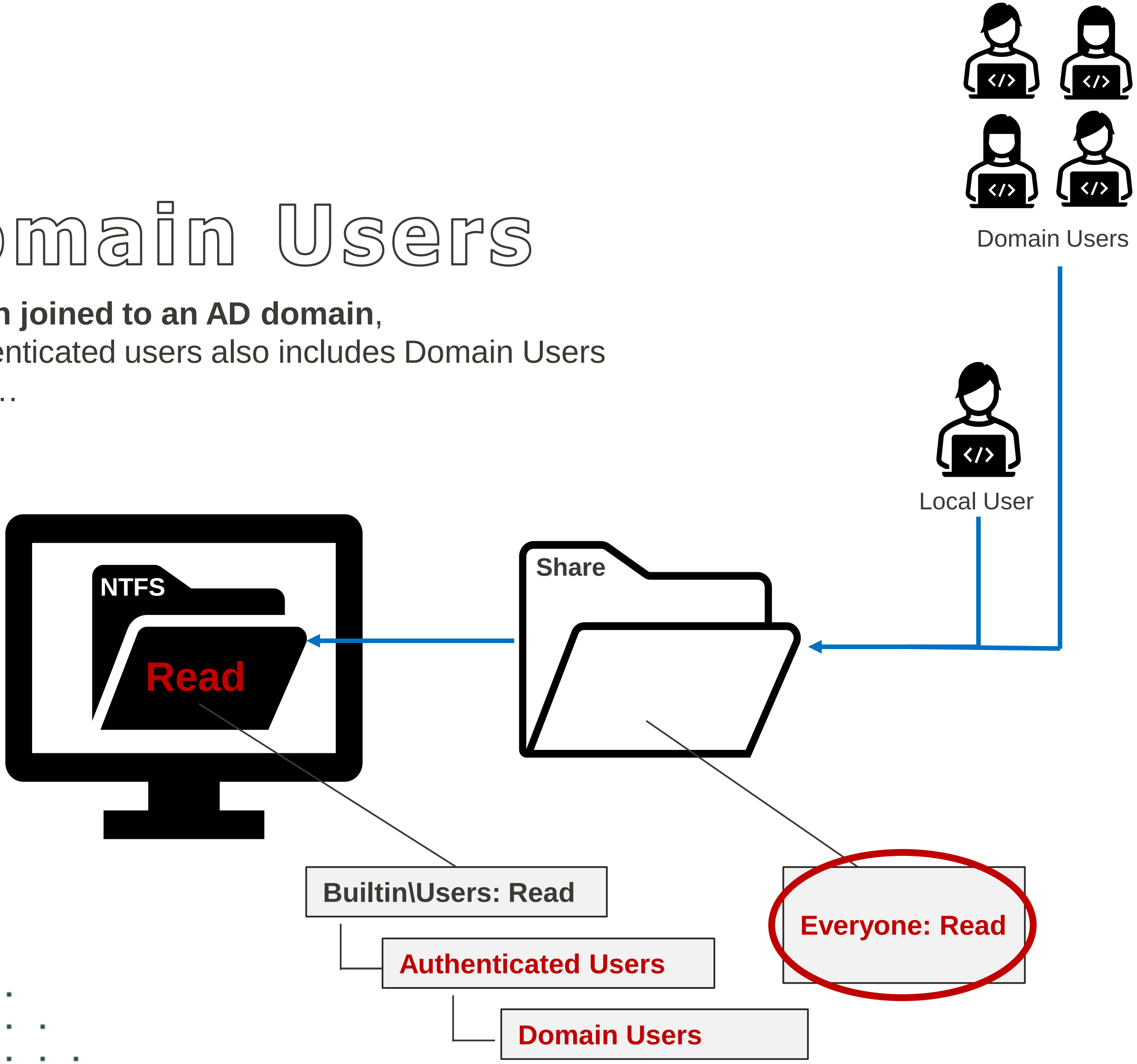
Share Permissions

- What's a share?
- Access control
- NTFS vs share priority

- Everyone
- Builtin\Users
- Authenticated Users
- Domain Users

Domain Users

When joined to an AD domain, authenticated users also includes Domain Users and …



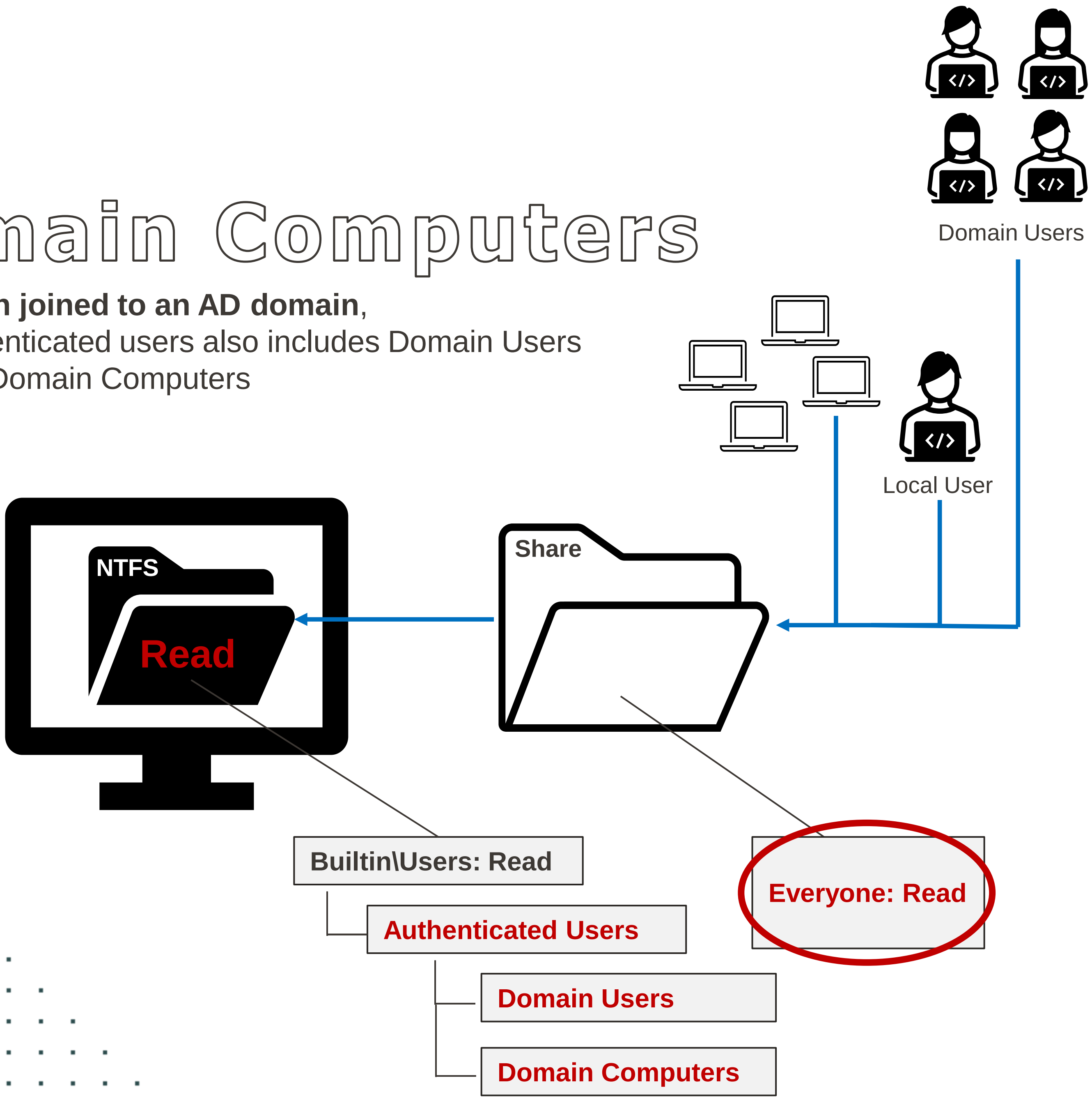
Share Permissions

- What's a share?
- Access control
- NTFS vs share priority

- Everyone
- Builtin\Users
- Authenticated Users
- Domain Users
- Domain Computers

Domain Computers

When joined to an AD domain, authenticated users also includes Domain Users and Domain Computers



Into the Abyss: Evaluating Active Directory SMB Shares on Scale

What’s the Impact?

Exploiting SMB Share Access!

NETSPI™

Impact
Share Exploitation

- **Share targeting**

Share Targeting

Permissions

Review change, write, and full control for broad groups.
- Everyone
- Builtin\Users
- Authenticated Users
- Domain Users
- Domain Computers
- Large nested groups

Data Exfiltration

- File names (password, pci, etc)
- File extensions (.sql, .bak, .ps1, etc)

Data Modification

- Change information to get paid
- Account number, approval etc

Lateral Movement & RCE

- c$ and admin$
- webroot / inetpub / www
- Auto runs

NETSPI™

Impact

Share Exploitation

- Share targeting
- Walkthrough: Read Access

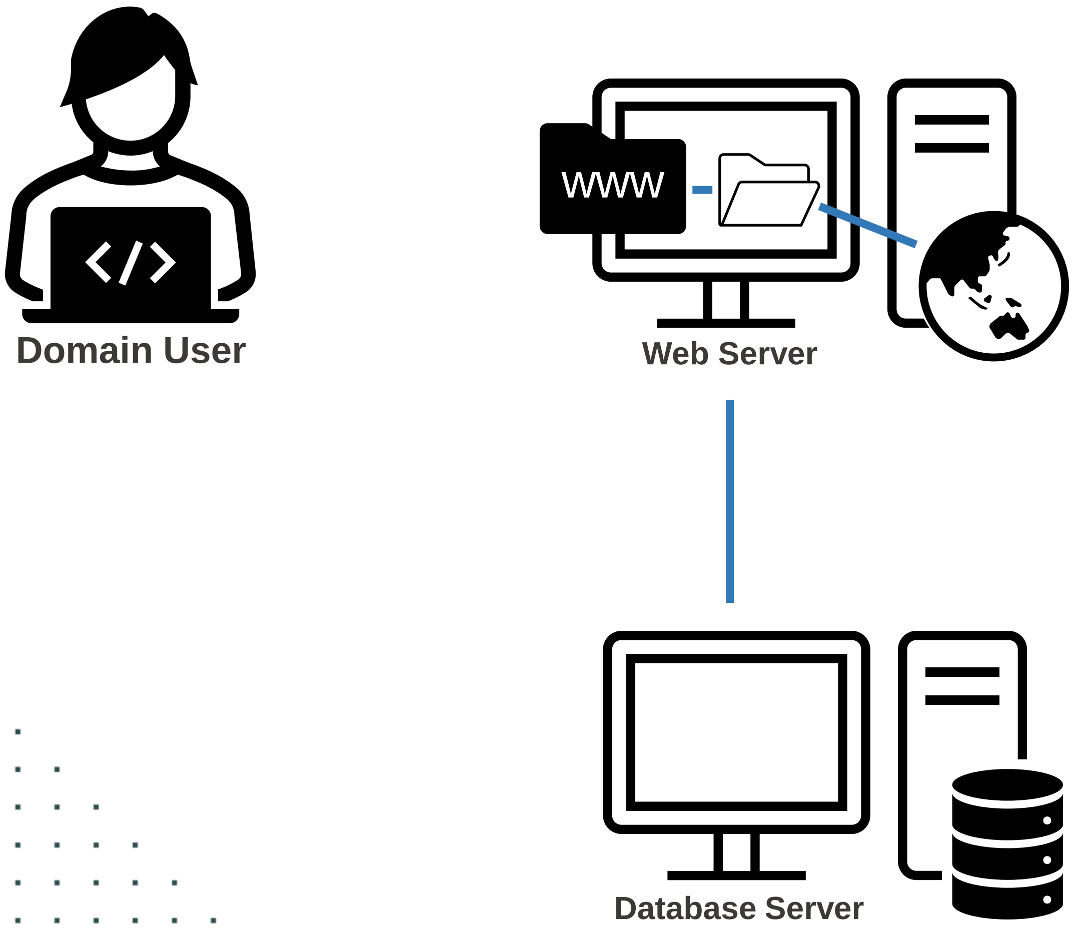
Share Exploitation Walkthrough

READ ACCESS

Impact

Share Exploitation

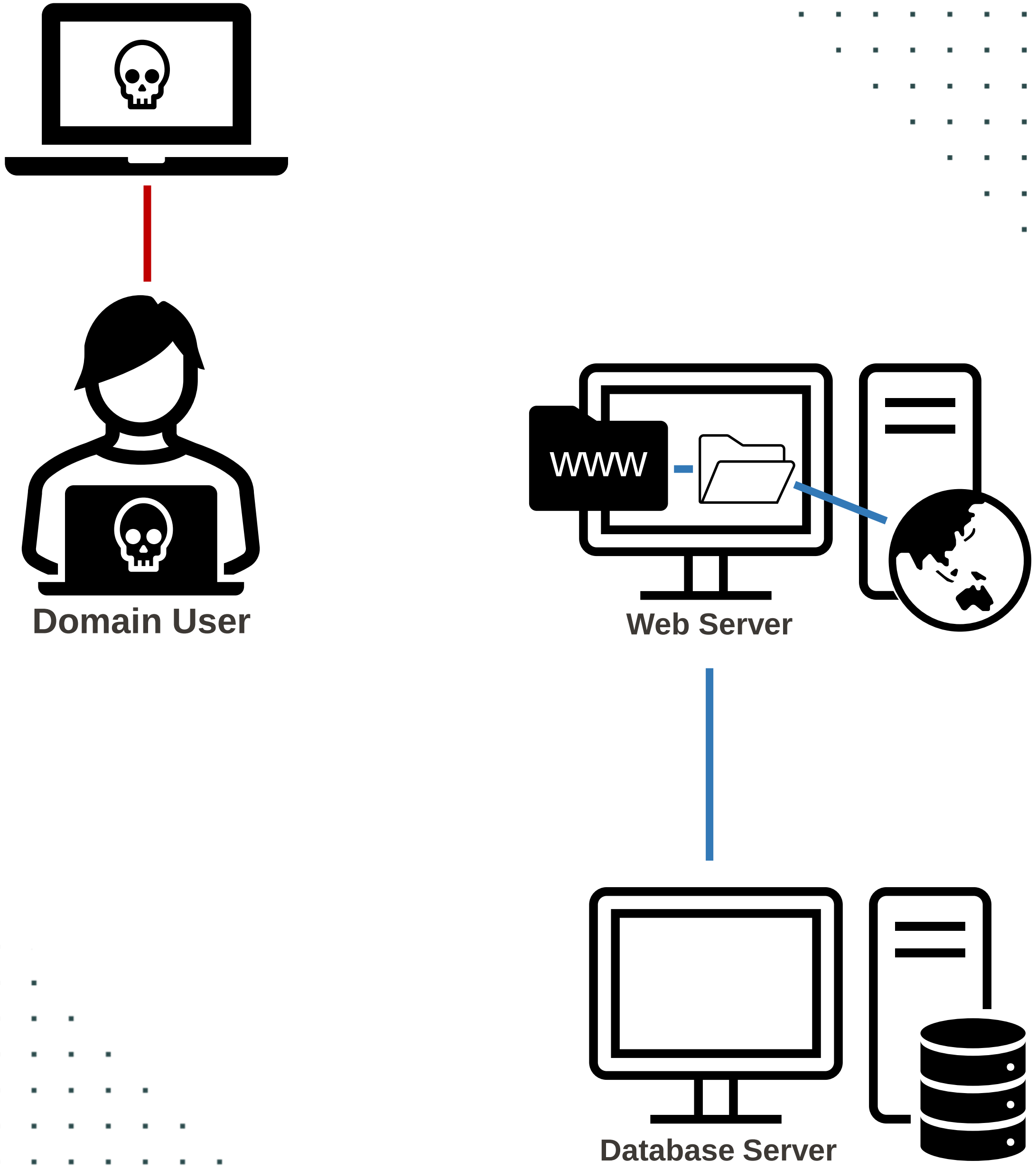
- **Share targeting**
- **Walkthrough: Read Access**



Impact

Share Exploitation

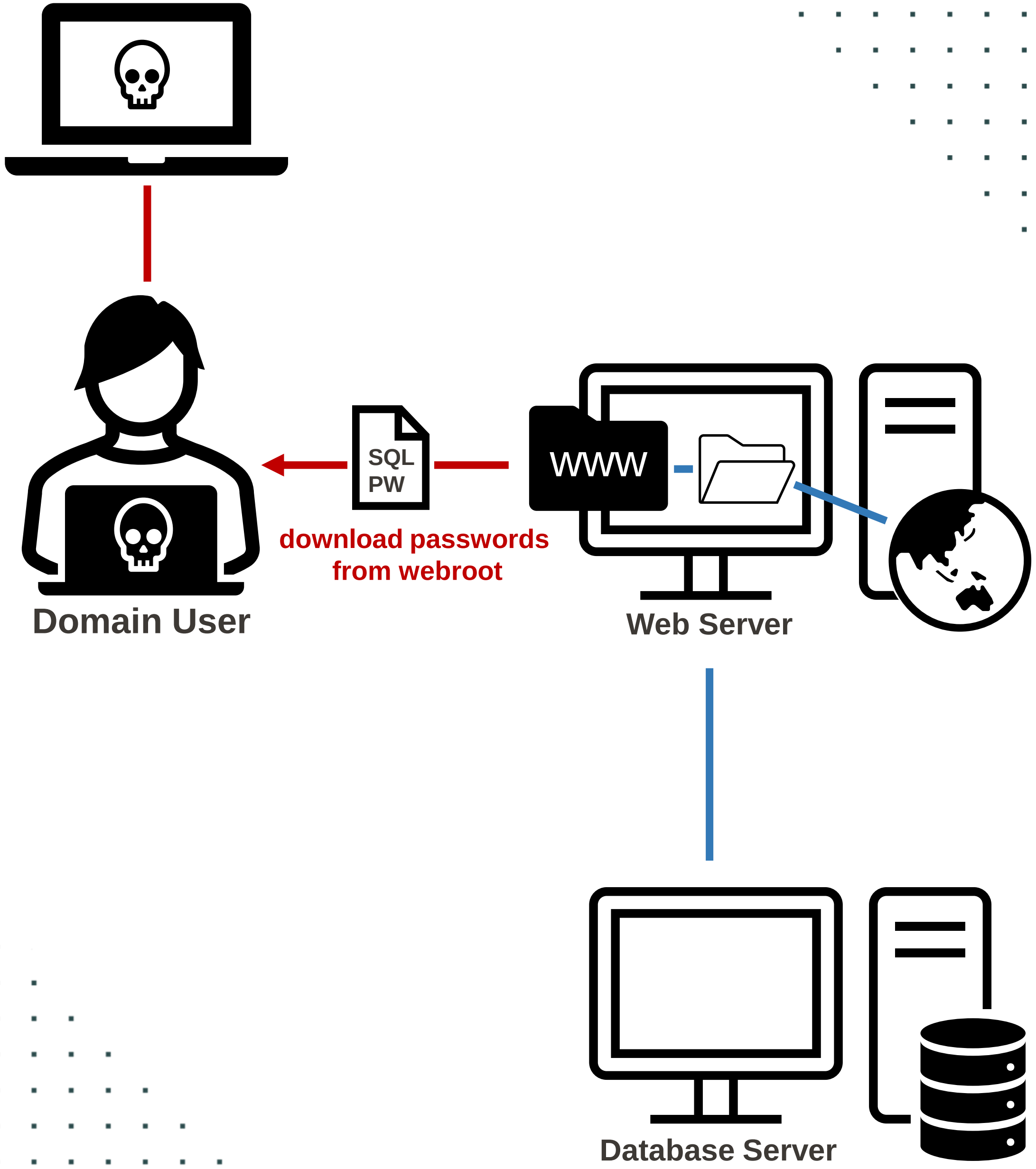
- **Share targeting**
- **Walkthrough: Read Access**



Impact

Share Exploitation

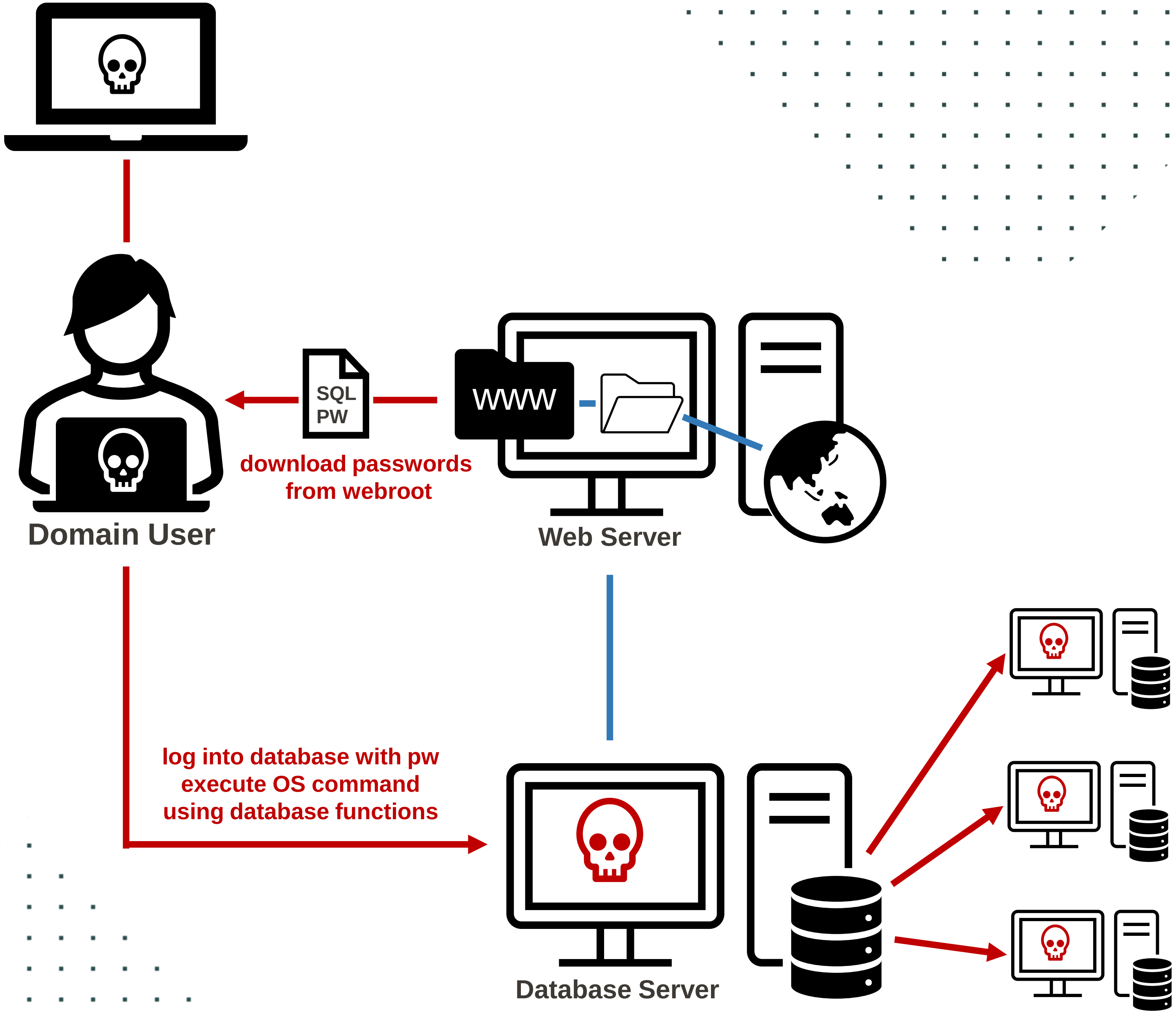
- Share targeting
- Walkthrough: Read Access



Impact

Share Exploitation

- Share targeting
- Walkthrough: Read Access



Impact

Share Exploitation

- Share targeting
- Walkthrough: Read Access
- Walkthrough: Write Access

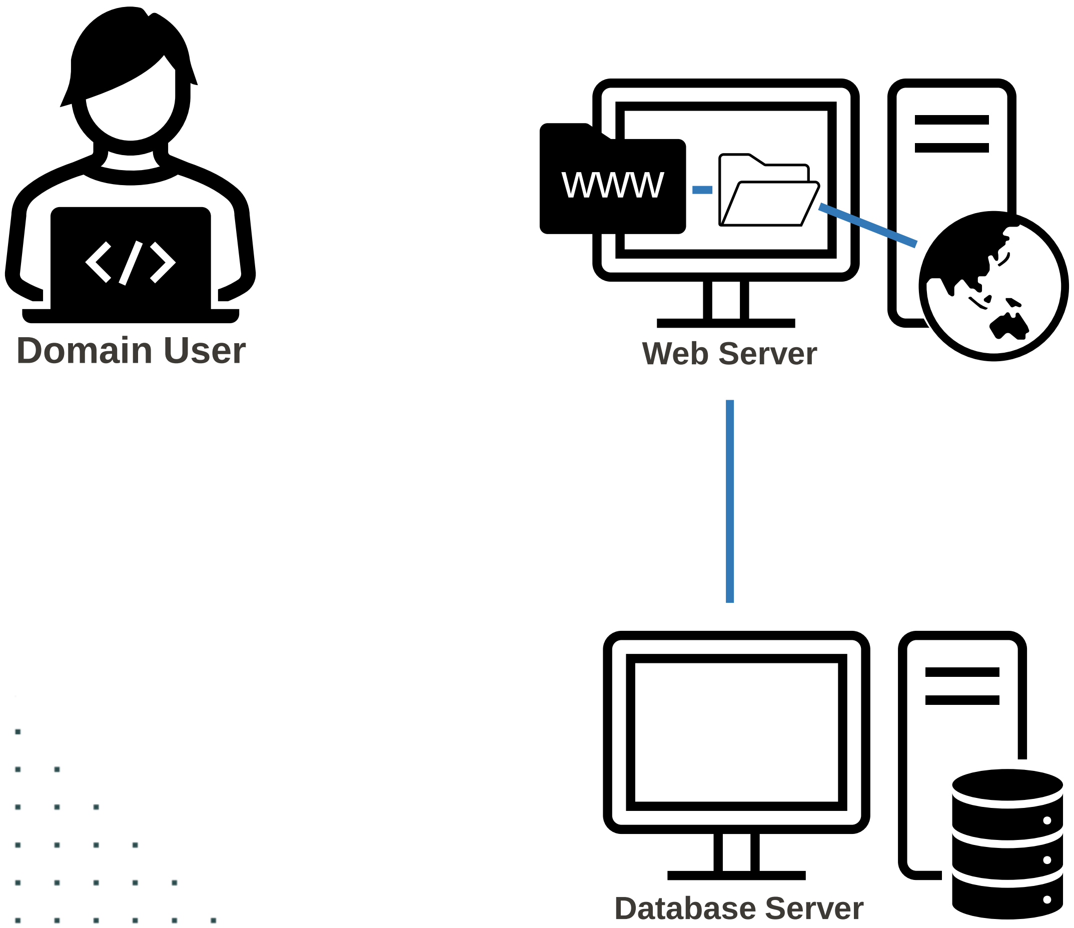
Share Exploitation Walkthrough

WRITE ACCESS

Impact

Share Exploitation

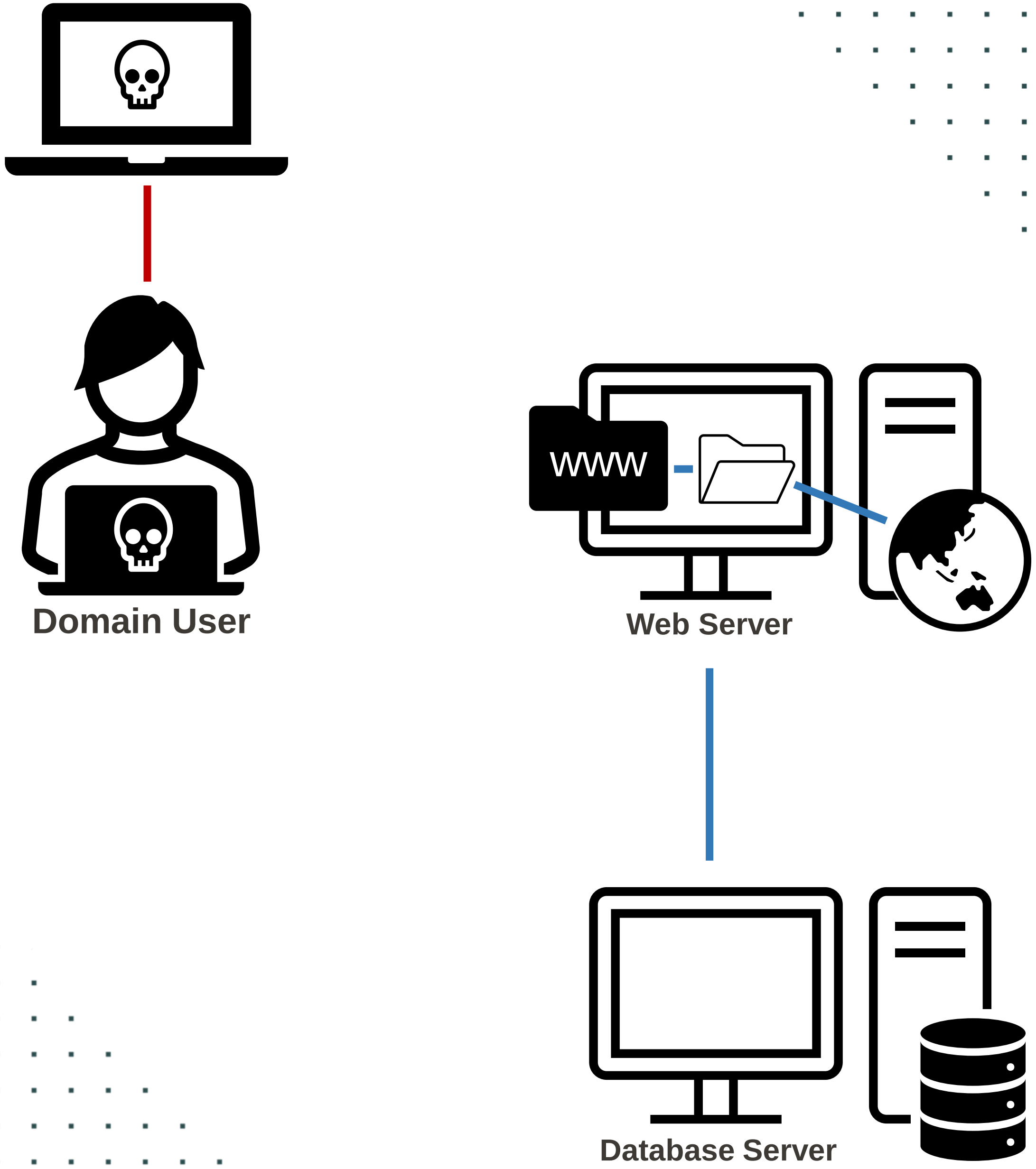
- Share targeting
- Walkthrough: Read Access
- Walkthrough: Write Access



Impact

Share Exploitation

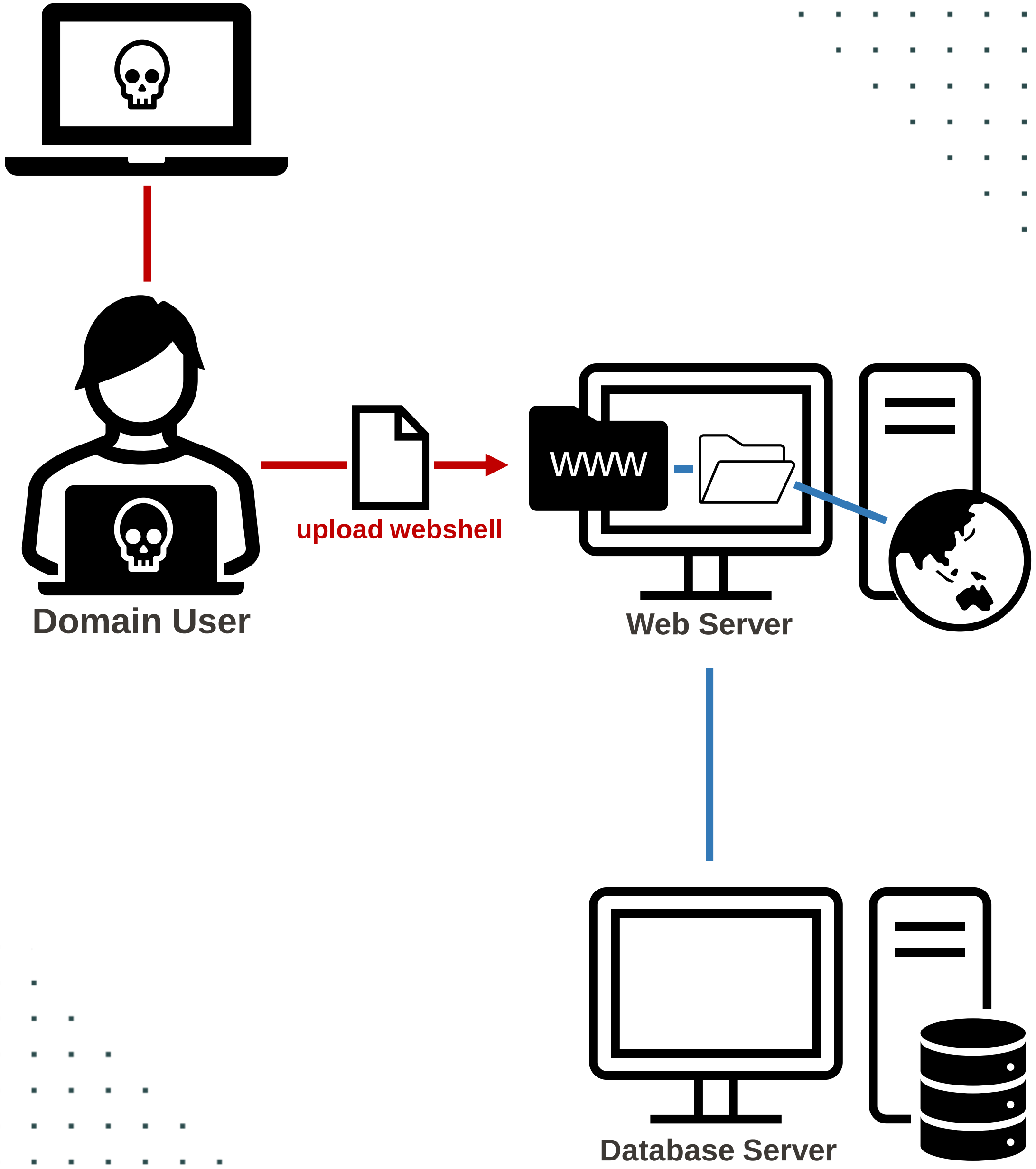
- Share targeting
- Walkthrough: Read Access
- Walkthrough: Write Access



Impact

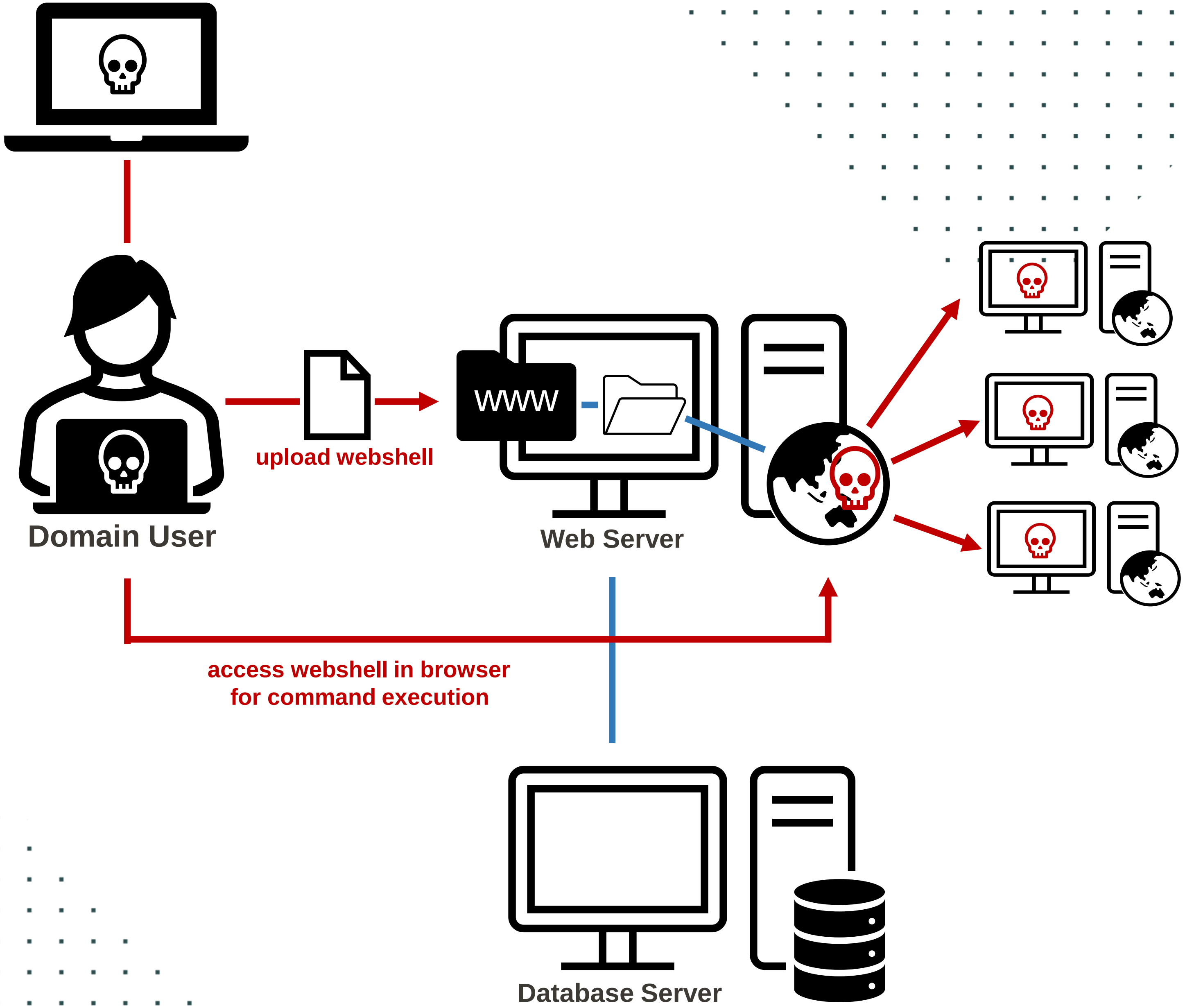
Share Exploitation

- Share targeting
- Walkthrough: Read Access
- Walkthrough: Write Access



Impact
Share Exploitation

- Share targeting
- Walkthrough: Read Access
- Walkthrough: Write Access



Impact

Share Exploitation

- Share targeting
- Walkthrough: Read Access
- Walkthrough: Write Access
- Walkthrough: More RCE Examples

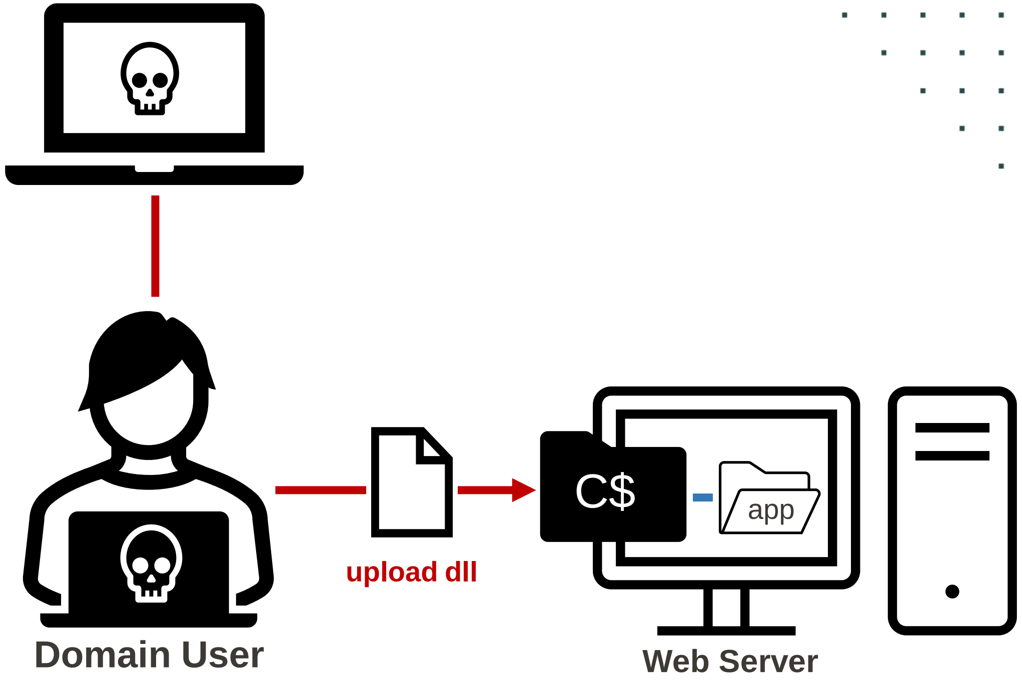
Share Exploitation Walkthrough

More RCE Examples

Impact

Share Exploitation

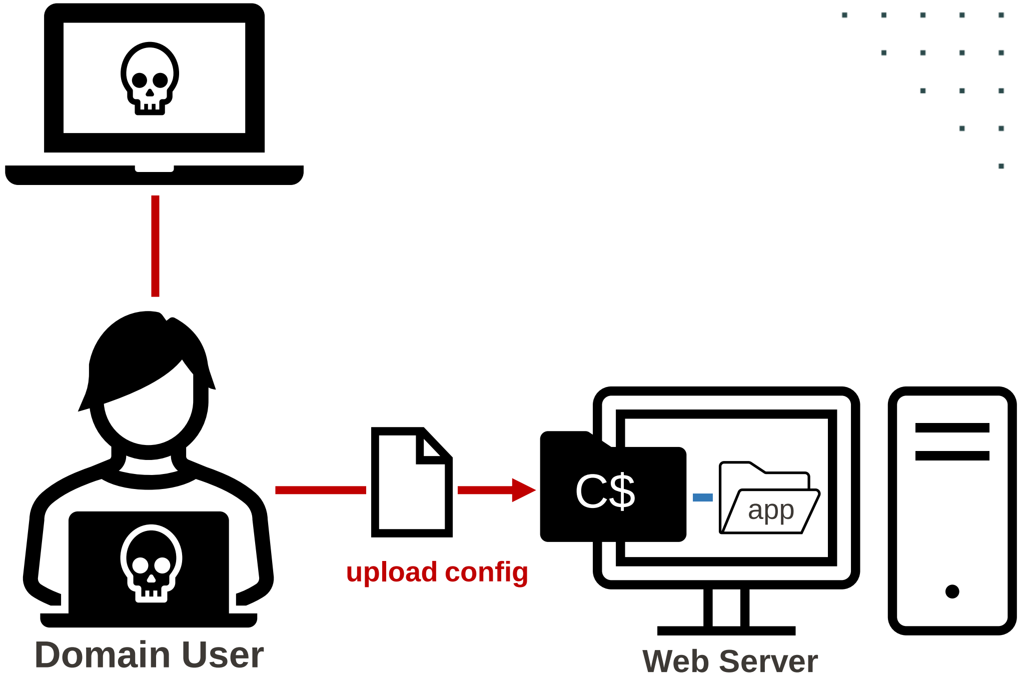
- Share targeting
- Share exploitation
- Walkthrough: Read Access
- Walkthrough: Write Access
- Walkthrough: RCE Examples



Application DLL Hijacking

Impact
Share Exploitation

- Share targeting
- Share exploitation
- Walkthrough: Read Access
- Walkthrough: Write Access
- Walkthrough: RCE Examples

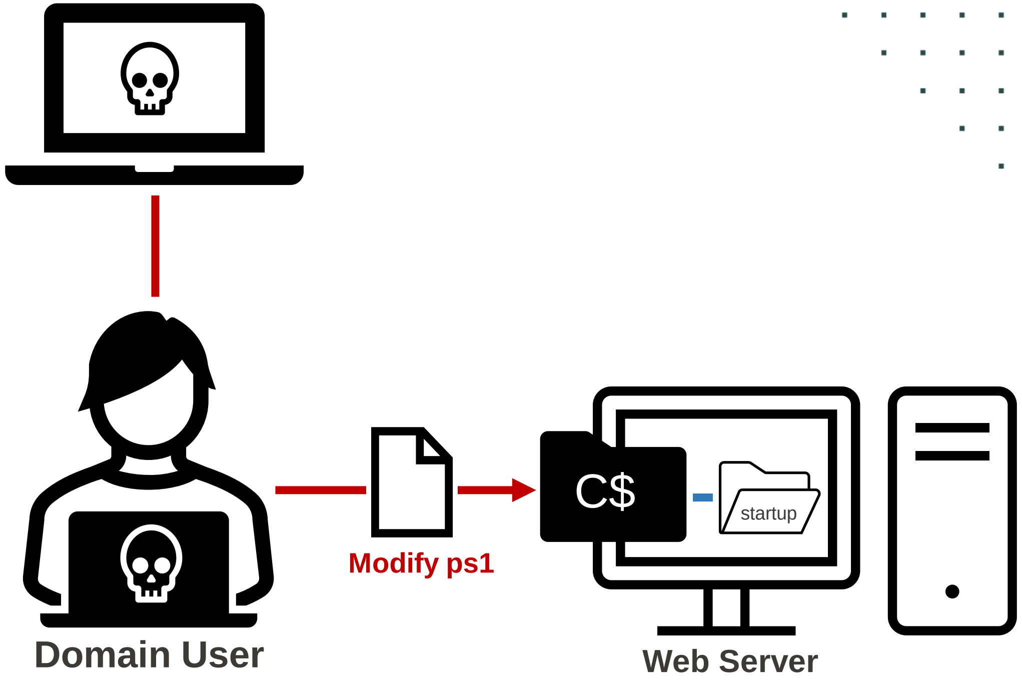


Application DLL Hijacking
Application Domain Hijacking

Impact

Share Exploitation

- Share targeting
- Share exploitation
- Walkthrough: Read Access
- Walkthrough: Write Access
- Walkthrough: RCE Examples



Application DLL Hijacking

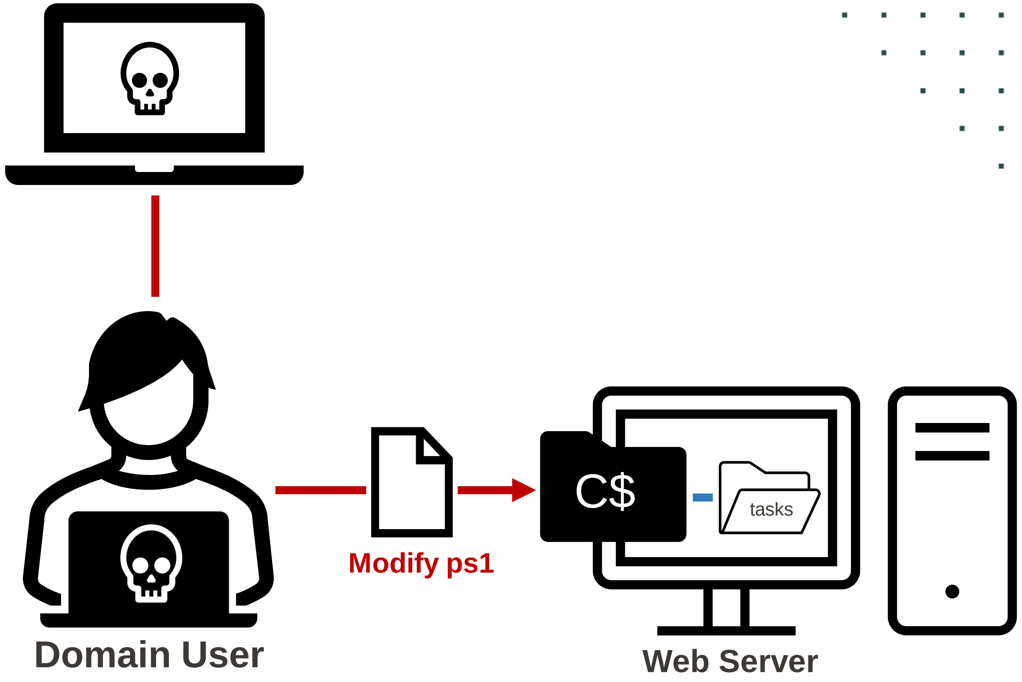
Application Domain Hijacking

All Users Startup

Impact

Share Exploitation

- Share targeting
- Share exploitation
- Walkthrough: Read Access
- Walkthrough: Write Access
- Walkthrough: RCE Examples

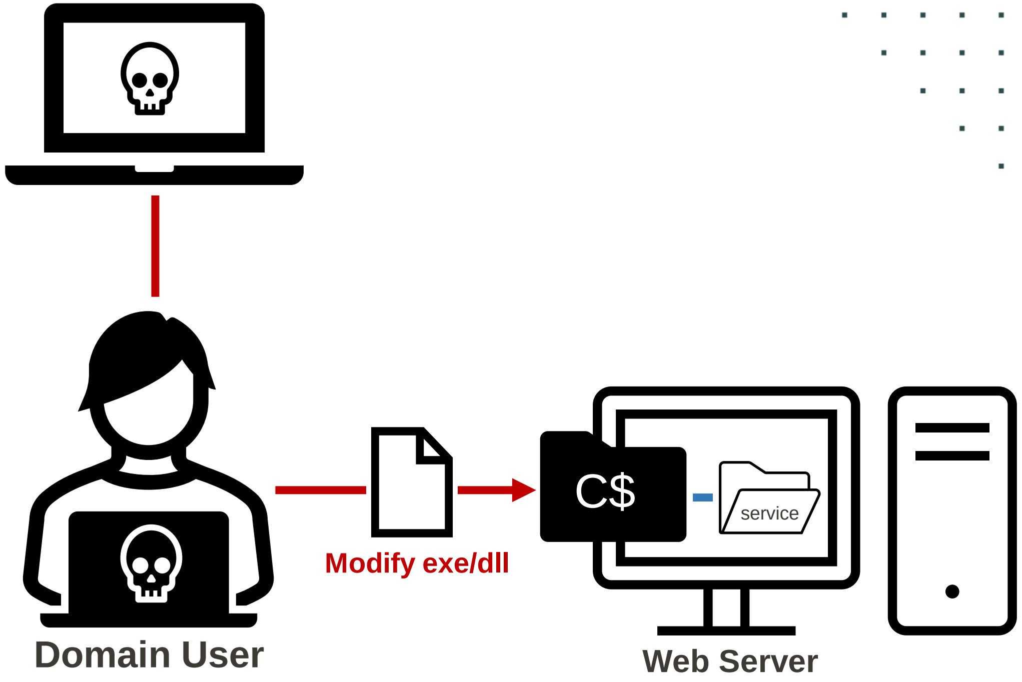


Application DLL Hijacking
Application Domain Hijacking
All Users Startup
Modify schedule task files

Impact

Share Exploitation

- Share targeting
- Share exploitation
- Walkthrough: Read Access
- Walkthrough: Write Access
- Walkthrough: RCE Examples



Application DLL Hijacking

Application Domain Hijacking

All Users Startup

Modify schedule task files

Modify service binaries

Into the Abyss: Evaluating Active Directory SMB Shares on Scale

Share Remediation

How can we streamline share inventory and remediation?

NETSPI™

Share Remediation

- **The challenge**

The Challenge

Remediating Share ACLs configured with excessive privileges

1	is easy
100	is manageable
1,000	is a pain
>100,000	seems unmanageable

NETSPI™

Share Remediation

- **The challenge**
- **Determine questions**

Determine Questions…

What do you need to know in order to streamline ACL fixes?

Where is the share (systems & subnets)?

What shares are high risk?

Who created the share?

When was it created?

What is it associated with (apps, process, BU)?

How common is the share in the environment?

Share Remediation

- The challenge
- Determine questions
- Identify data sources

Identify Data sources...

Where can you Get the data you need?

Active Directory computers and subnets

Share owners and creation dates / times

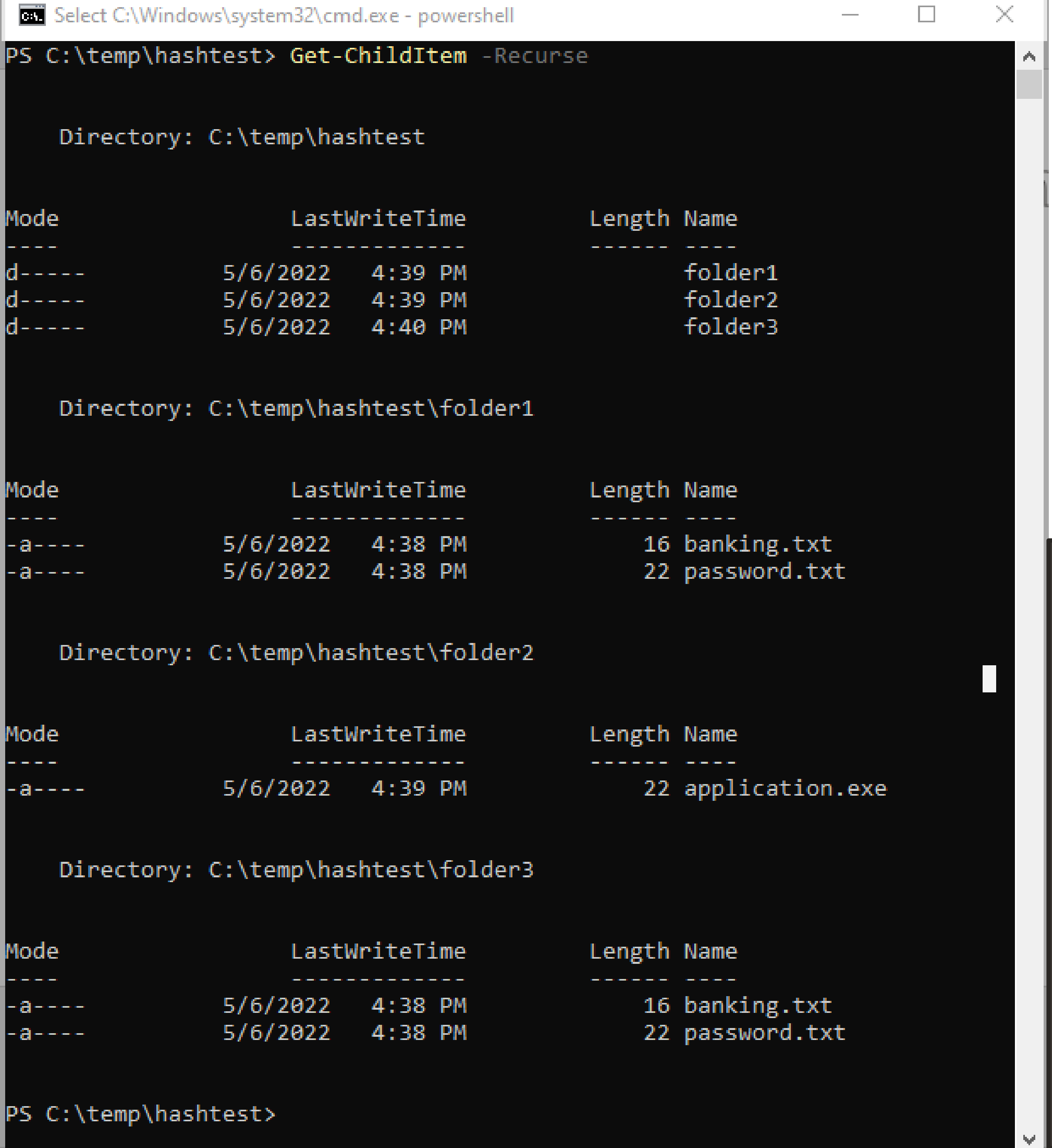
Share names, folders, files, counts, ACLs, list hash

CMDB for assets owners and context

Share Remediation

- The challenge
- Determine questions
- Identify data sources

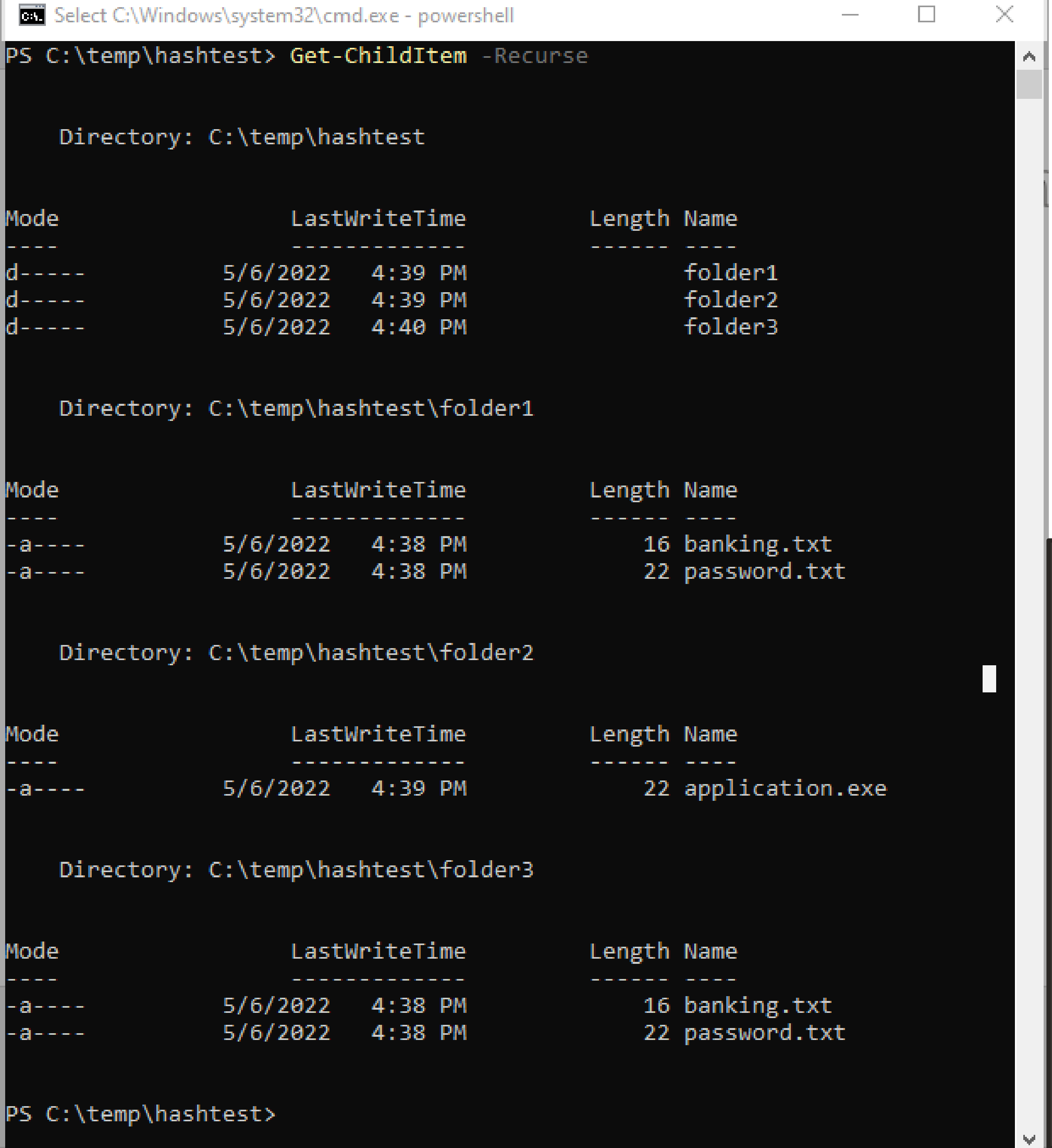
Comparing& grouping Folder list hashes



```
PS C:\temp\hashtest> Get-ChildItem -Recurse


    Directory: C:\temp\hashtest


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/6/2022   4:39 PM                folder1
d-----          5/6/2022   4:39 PM                folder2
d-----          5/6/2022   4:40 PM                folder3


    Directory: C:\temp\hashtest\folder1


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/6/2022   4:38 PM             16 banking.txt
-a----          5/6/2022   4:38 PM             22 password.txt


    Directory: C:\temp\hashtest\folder2


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/6/2022   4:39 PM             22 application.exe


    Directory: C:\temp\hashtest\folder3


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/6/2022   4:38 PM             16 banking.txt
-a----          5/6/2022   4:38 PM             22 password.txt


PS C:\temp\hashtest>
```

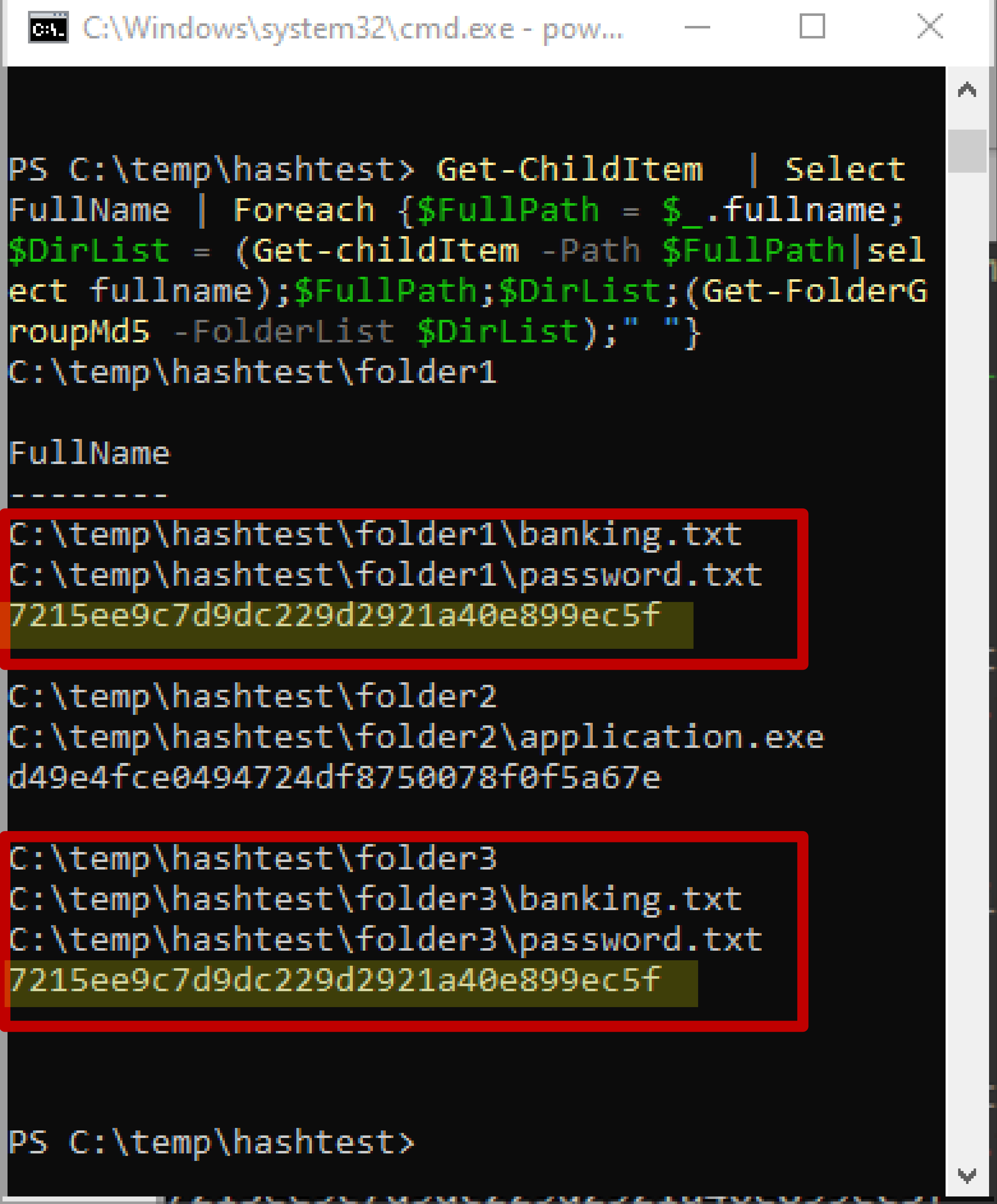
3 Directories
2 contain the same files

How can we identify those Grouping on scale?

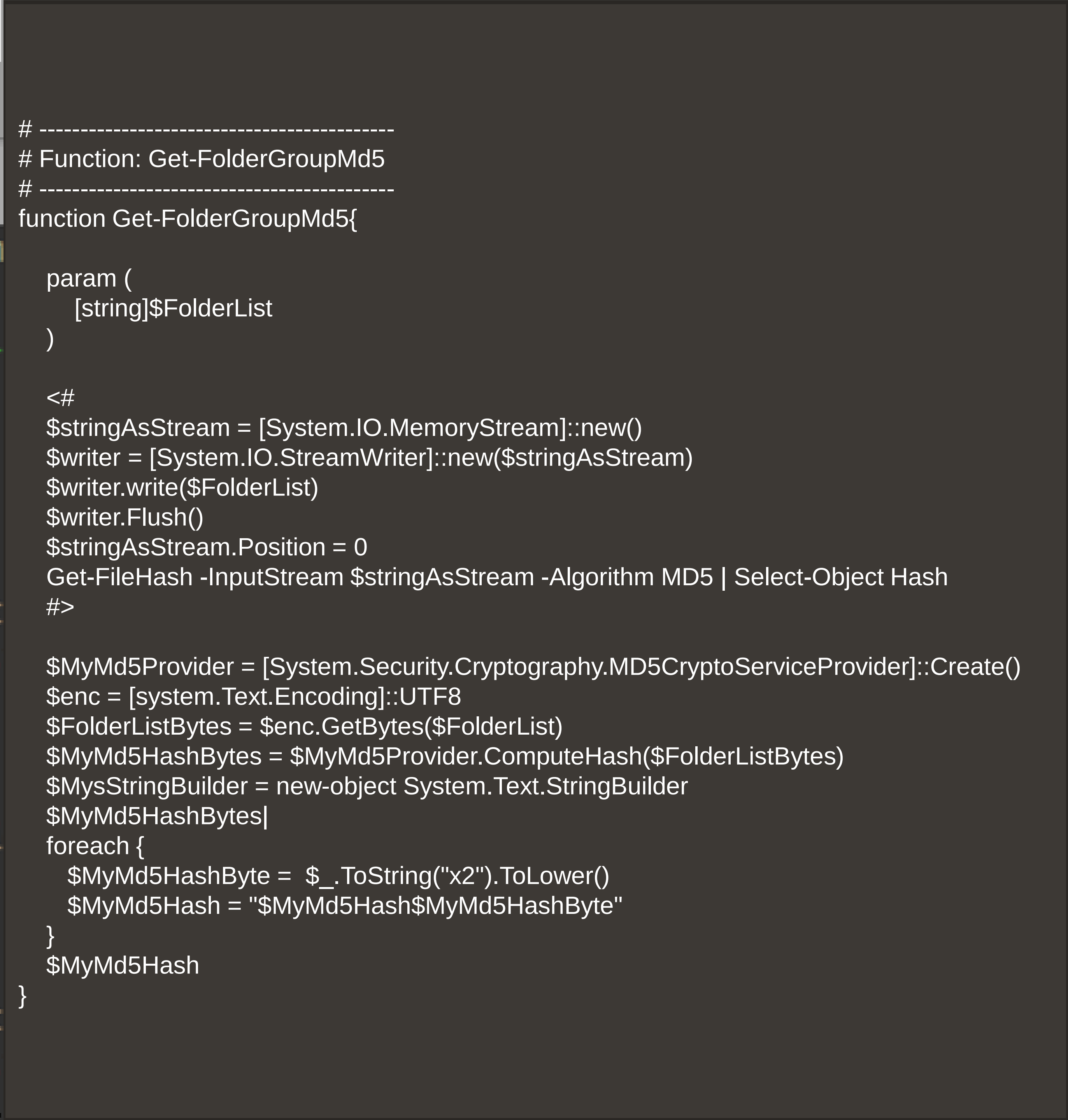


```
PS C:\temp\hashtest> Get-ChildItem -Recurse


    Directory: C:\temp\hashtest


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          5/6/2022   4:39 PM                folder1
d-----          5/6/2022   4:39 PM                folder2
d-----          5/6/2022   4:40 PM                folder3


    Directory: C:\temp\hashtest\folder1


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/6/2022   4:38 PM             16 banking.txt
-a----          5/6/2022   4:38 PM             22 password.txt


    Directory: C:\temp\hashtest\folder2


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/6/2022   4:39 PM             22 application.exe


    Directory: C:\temp\hashtest\folder3


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          5/6/2022   4:38 PM             16 banking.txt
-a----          5/6/2022   4:38 PM             22 password.txt


PS C:\temp\hashtest>
```

Directory List Hashing



```
PS C:\temp\hashtest> Get-ChildItem  | Select
FullName | Foreach {$FullPath = $_.fullname;
$DirList = (Get-childItem -Path $FullPath|sel
ect fullname);$FullPath;$DirList;(Get-FolderG
roupMd5 -FolderList $DirList);" "}
C:\temp\hashtest\folder1

FullName
--------
C:\temp\hashtest\folder1\banking.txt
C:\temp\hashtest\folder1\password.txt
7215ee9c7d9dc229d2921a40e899ec5f

C:\temp\hashtest\folder2
C:\temp\hashtest\folder2\application.exe
d49e4fce0494724df8750078f0f5a67e

C:\temp\hashtest\folder3
C:\temp\hashtest\folder3\banking.txt
C:\temp\hashtest\folder3\password.txt
7215ee9c7d9dc229d2921a40e899ec5f


PS C:\temp\hashtest>
```



```
# --------------------------------------------
# Function: Get-FolderGroupMd5
# --------------------------------------------
function Get-FolderGroupMd5{

    param (
        [string]$FolderList
    )

    <#
    $stringAsStream = [System.IO.MemoryStream]::new()
    $writer = [System.IO.StreamWriter]::new($stringAsStream)
    $writer.write($FolderList)
    $writer.Flush()
    $stringAsStream.Position = 0
    Get-FileHash -InputStream $stringAsStream -Algorithm MD5 | Select-Object Hash
    #>

    $MyMd5Provider = [System.Security.Cryptography.MD5CryptoServiceProvider]::Create()
    $enc = [system.Text.Encoding]::UTF8
    $FolderListBytes = $enc.GetBytes($FolderList)
    $MyMd5HashBytes = $MyMd5Provider.ComputeHash($FolderListBytes)
    $MysStringBuilder = new-object System.Text.StringBuilder
    $MyMd5HashBytes|
    foreach {
       $MyMd5HashByte =  $_.ToString("x2").ToLower()
       $MyMd5Hash = "$MyMd5Hash$MyMd5HashByte"
    }
    $MyMd5Hash
}
```

Share Remediation

- The challenge
- Determine questions
- Identify data sources
- Data collection

PowerShell can be run unprivileged or with administrative privileges via PowerShell Remoting

Collect Required Data

How will you collect that data?

Active Directory

ldap queries for computer and subnet information.

Get-ADComputer, Get-ADReplicationSubnet, Powerview

Shares

RPC calls for share and file information.

Get-SMBShare, Get-SmbShareAccess, Get-ACL, Powerview

Share Remediation

- **The challenge**
- **Determine questions**
- **Identify data sources**
- **Data collection**

Collect Required Data

Quick Tips

Active Directory

LDAP queries can provide a list of all domain computers

1 Include all domains

2 Verify domain user privileges

3 Ping & Port scan to understand potential connectivity issues

Port Scanning

TCP 445 across known subnets

1 Make sure you have a complete inventory of your subnets

2 Make sure you are not being blocked by firewalls

Share Remediation

- The challenge
- Determine questions
- Identify data sources
- Data collection
- Data Analysis

Data Analysis

Start grouping data to answer questions!

What shares are high risk?

Who created the share?

When was it created?

Where was it created (systems & subnets)?

What is it associated with (apps, process, BU)?

How common is the share in the environment?

Share Remediation

- The challenge
- Determine questions
- Identify data sources
- Data collection
- Data Analysis

Data Analysis

Basic Techniques

Search for known high risk share names

Group/Count owners, names, subnets, files, acls

Timeline analysis to find patterns

Share Remediation

- The challenge
- Determine questions
- Identify data sources
- Data collection
- Data Analysis
- Data interpretation
- Prioritize remediation

Reference owner, subnet computer object, & timeline for additional context

Prioritizing Triage

1 **Filter for ACLs assigned to inherited groups**

2 **Review high risk shares**

3 **Group shares by <u>name</u>**
Count, context, write read

4 **Group shares by <u>folder list</u>**
Count, context, write read

5 **Cross Reference CMDB**
Count, context, write read

NETSPI™

Share Remediation

- The challenge
- Determine questions
- Identify data sources
- Data collection
- Data Analysis
- Data interpretation
- Prioritize remediation

These techniques are not perfect
but they will help reduce effort during remediation

Into the Abyss: Evaluating Active Directory SMB Shares on Scale

Recommendations

NETSPI™

Recommendations

- Preventative measures

Preventative Measures

Administrative Controls

- Policies
- Standards
- Procedures
- Change control
- **Least privilege**
- **Attack Surface Reduction**

Isolation

- Network
- Host-based

NETSPI™

Recommendations

- **Preventative measures**
- **Detective measures**

Detective Measures

Monitor Share Inventory

- Monitor high value shares for changes
- Perform your own discovery and analysis on a regular basis (ideally quarterly)

Monitor for Share Scanning

- Port 445 scanning
  Netflow data
- Authenticated scanning
  Event IDs: 540, 4624, 680,4625
- Share scanning
  Event ID: 5140

Recommendations

- Preventative measures
- Detective measures
- Corrective measures

Corrective Measures

Track and Remediate Excessive Privileges

- Make sure you have a system in place to track the share exposure and fixes over time.
- Treat them like a vulnerability.
- Assign a ticket to the owner of the system or application so the fixes can be tracked.

NETSPI™

Into the Abyss: Evaluating Active Directory SMB Shares on Scale

PowerHuntShares

Automate High Risk Shares Identification

NETSPI™

PowerHuntShares

Inventory Share Access

in Active Directory environments automatically

Identify HIGH RISK Shares

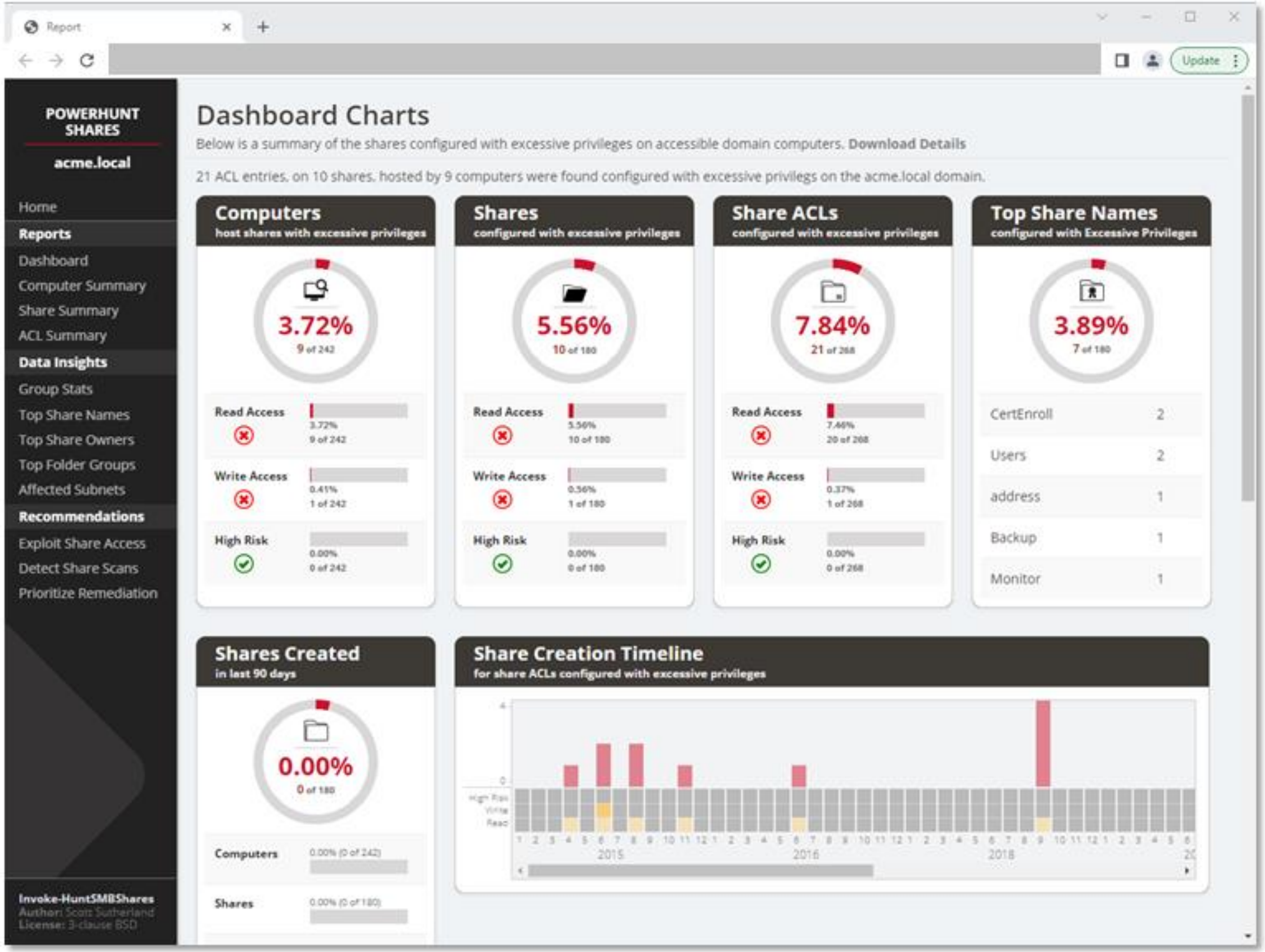
based on common names, files, and privileges

Prioritize Remediation

using environment specific analytics

DOWNLOAD IT:
https://github.com/NetSPI/PowerHuntShares

NETSPI™



POWERHUNT SHARES

acme.local

- Home
- **Reports**
- Dashboard
- Computer Summary
- Share Summary
- ACL Summary
- **Data Insights**
- Group Stats
- Top Share Names
- Top Share Owners
- Top Folder Groups
- Affected Subnets
- **Recommendations**
- Exploit Share Access
- Detect Share Scans
- Prioritize Remediation

Invoke-HuntSMBShares
Author: Scott Sutherland
License: 3-clause BSD

Dashboard Charts

Below is a summary of the shares configured with excessive privileges on accessible domain computers. **Download Details**

21 ACL entries, on 10 shares, hosted by 9 computers were found configured with excessive privilegs on the acme.local domain.

Computers
host shares with excessive privileges

3.72%
9 of 242

Read Access ☒	3.72% 9 of 242
Write Access ☒	0.41% 1 of 242
High Risk ✓	0.00% 0 of 242

Shares
configured with excessive privileges

5.56%
10 of 180

Read Access ☒	5.56% 10 of 180
Write Access ☒	0.56% 1 of 180
High Risk ✓	0.00% 0 of 180

Share ACLs
configured with excessive privileges

7.84%
21 of 268

Read Access ☒	7.46% 20 of 268
Write Access ☒	0.37% 1 of 268
High Risk ✓	0.00% 0 of 268

Top Share Names
configured with Excessive Privileges

3.89%
7 of 180

CertEnroll	2
Users	2
address	1
Backup	1
Monitor	1

Shares Created
in last 90 days

0.00%
0 of 180

Computers	0.00% (0 of 242)
Shares	0.00% (0 of 180)

Share Creation Timeline
for share ACLs configured with excessive privileges

NETSPI™
Open-Source Software

PowerHuntShares

- **Installation**

Installation: Option 1

Download & Import

```
https://github.com/NetSPI/PowerHuntShares/
```

Import

```
Import-Module PowerHuntShares.psm1
```

PowerHuntShares

- **Installation**

Installation: Option 2

Download & Load into Memory

```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
[Net.ServicePointManager]::SecurityProtocol =[Net.SecurityProtocolType]::Tls12

IEX(New-Object System.Net.WebClient).DownloadString("https://raw.githubusercontent.com/NetSPI/PowerHuntShares/main/PowerHuntShares.psm1")
```

PowerHuntShares

- **Installation**
- **Execution**

Execution

Run from domain joined system

```
Invoke-HuntSMBShares -Threads 100 -OutputDirectory c:\temp\test
```

Run from a non-domain joined system

```
runas /netonly /user:domain\user PowerShell.exe

Invoke-HuntSMBShares -Threads 100 -RunSpaceTimeOut 10 -
OutputDirectory c:\folder\ -DomainController 10.1.1.1 -Credential
domain\user
```

PowerHuntShares

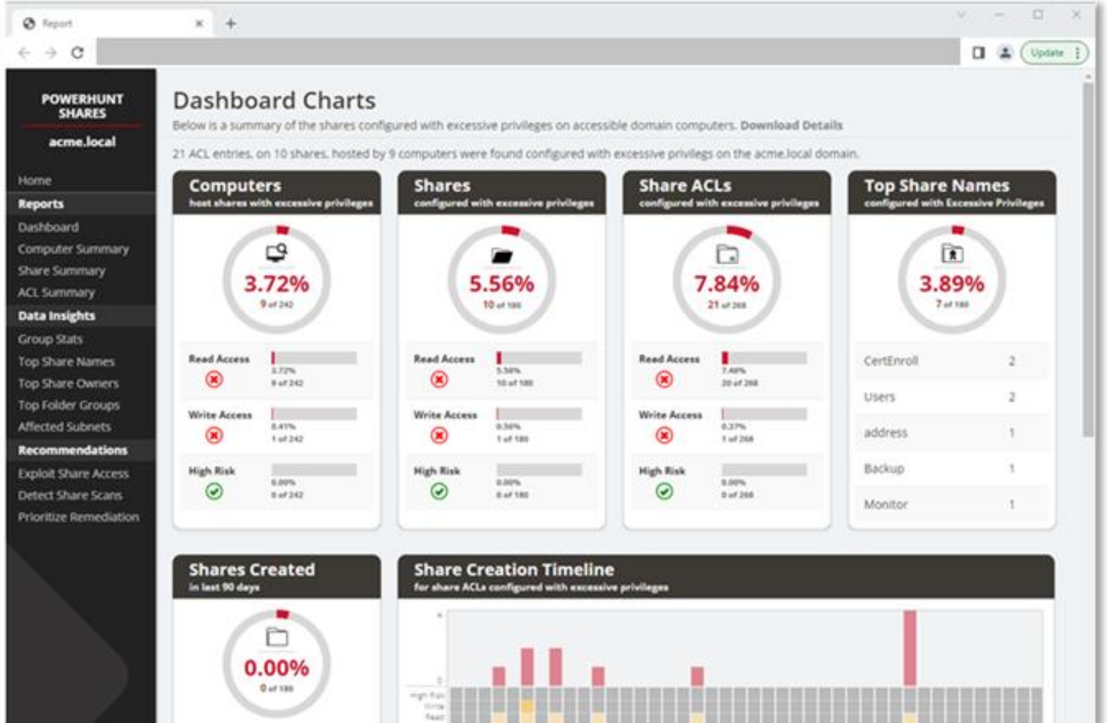
- Installation
- Execution
- Reporting

NETSPI™

Report

HTML Report

review result summary and data insights to help drive remediation.



POWERHUNT SHARES

acme.local

Home

Reports

Dashboard

Computer Summary

Share Summary

ACL Summary

Data Insights

Group Stats

Top Share Names

Top Share Owners

Top Folder Groups

Affected Subnets

Recommendations

Exploit Share Access

Detect Share Scans

Prioritize Remediation

Dashboard Charts

Below is a summary of the shares configured with excessive privileges on accessible domain computers. **Download Details**

21 ACL entries, on 10 shares, hosted by 9 computers were found configured with excessive privilegs on the acme.local domain.

Computers
host shares with excessive privileges

3.72%
9 of 242

Read Access ☒ 3.72% 9 of 242

Write Access ☒ 0.41% 1 of 242

High Risk ✓ 0.00% 0 of 242

Shares
configured with excessive privileges

5.56%
10 of 180

Read Access ☒ 5.56% 10 of 180

Write Access ☒ 0.56% 1 of 180

High Risk ✓ 0.00% 0 of 180

Share ACLs
configured with excessive privileges

7.84%
21 of 268

Read Access ☒ 7.46% 20 of 268

Write Access ☒ 0.37% 1 of 268

High Risk ✓ 0.00% 0 of 268

Top Share Names
configured with Excessive Privileges

3.89%
7 of 180

CertEnroll	2
Users	2
address	1
Backup	1
Monitor	1

Shares Created
in last 90 days

0.00%
0 of 180

Share Creation Timeline
for share ACLs configured with excessive privileges

PowerHuntShares

- Installation
- Execution
- Reporting

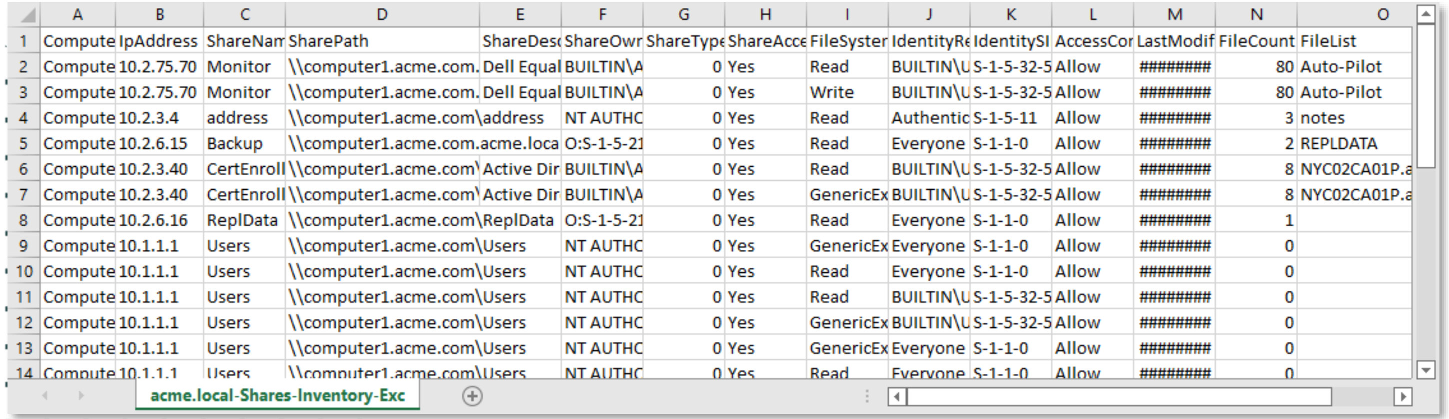
Report

HTML Report

review result summary and data insights to help drive remediation.

CSV Output

review potentially excessive share ACL entry details in the associated CSV files.

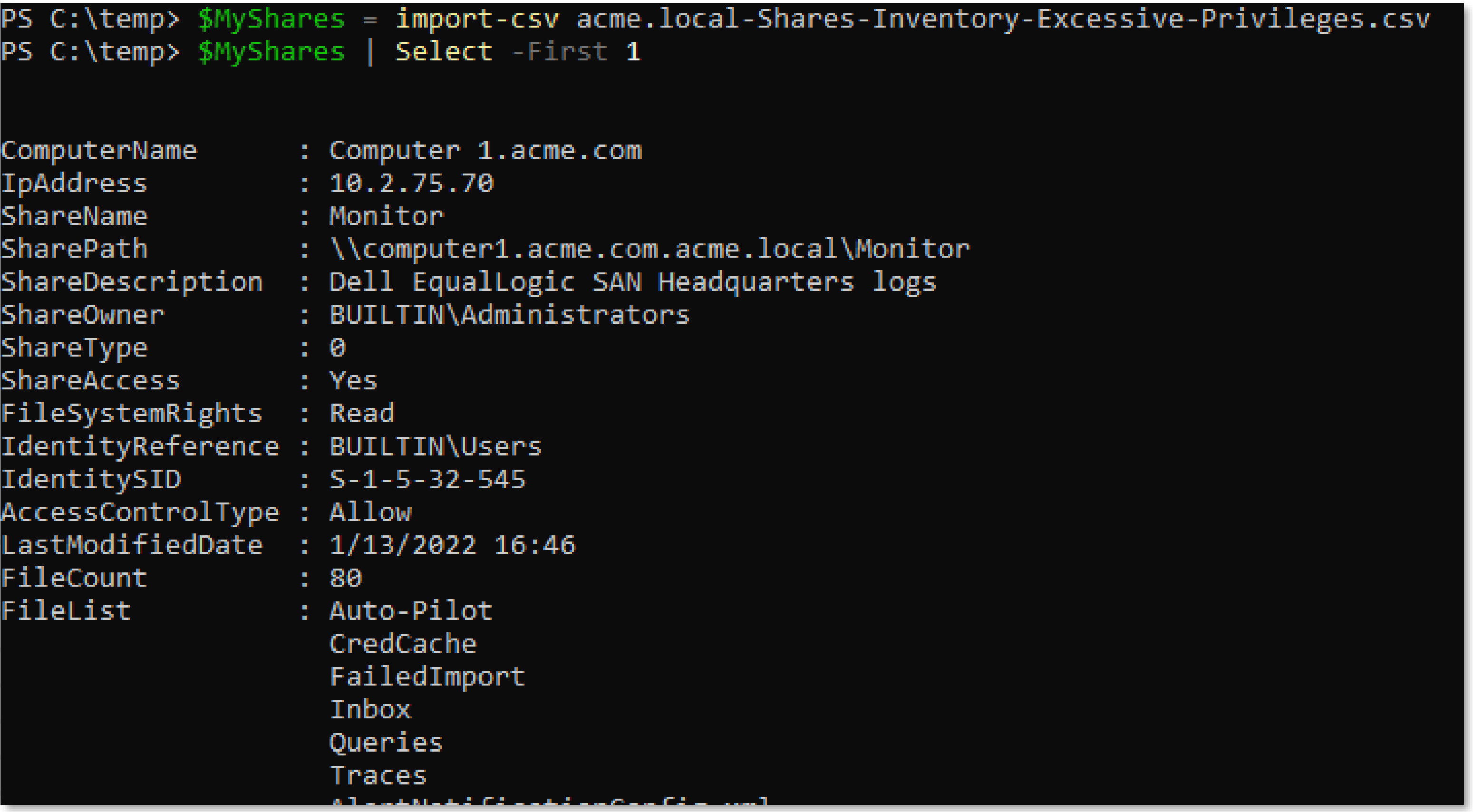


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Compute	IpAddress	ShareNam	SharePath	ShareDes	ShareOwr	ShareType	ShareAcce	FileSyster	IdentityRe	IdentitySI	AccessCor	LastModif	FileCount	FileList
2	Compute	10.2.75.70	Monitor	\\computer1.acme.com.	Dell Equal	BUILTIN\A	0	Yes	Read	BUILTIN\U	S-1-5-32-5	Allow	#########	80	Auto-Pilot
3	Compute	10.2.75.70	Monitor	\\computer1.acme.com.	Dell Equal	BUILTIN\A	0	Yes	Write	BUILTIN\U	S-1-5-32-5	Allow	#########	80	Auto-Pilot
4	Compute	10.2.3.4	address	\\computer1.acme.com\address		NT AUTHC	0	Yes	Read	Authentic	S-1-5-11	Allow	#########	3	notes
5	Compute	10.2.6.15	Backup	\\computer1.acme.com.acme.loca		O:S-1-5-21	0	Yes	Read	Everyone	S-1-1-0	Allow	#########	2	REPLDATA
6	Compute	10.2.3.40	CertEnroll	\\computer1.acme.com\	Active Dir	BUILTIN\A	0	Yes	Read	BUILTIN\U	S-1-5-32-5	Allow	#########	8	NYC02CA01P.a
7	Compute	10.2.3.40	CertEnroll	\\computer1.acme.com\	Active Dir	BUILTIN\A	0	Yes	GenericEx	BUILTIN\U	S-1-5-32-5	Allow	#########	8	NYC02CA01P.a
8	Compute	10.2.6.16	ReplData	\\computer1.acme.com\ReplData		O:S-1-5-21	0	Yes	Read	Everyone	S-1-1-0	Allow	#########	1	
9	Compute	10.1.1.1	Users	\\computer1.acme.com\Users		NT AUTHC	0	Yes	GenericEx	Everyone	S-1-1-0	Allow	#########	0	
10	Compute	10.1.1.1	Users	\\computer1.acme.com\Users		NT AUTHC	0	Yes	Read	Everyone	S-1-1-0	Allow	#########	0	
11	Compute	10.1.1.1	Users	\\computer1.acme.com\Users		NT AUTHC	0	Yes	Read	BUILTIN\U	S-1-5-32-5	Allow	#########	0	
12	Compute	10.1.1.1	Users	\\computer1.acme.com\Users		NT AUTHC	0	Yes	GenericEx	BUILTIN\U	S-1-5-32-5	Allow	#########	0	
13	Compute	10.1.1.1	Users	\\computer1.acme.com\Users		NT AUTHC	0	Yes	GenericEx	Everyone	S-1-1-0	Allow	#########	0	
14	Compute	10.1.1.1	Users	\\computer1.acme.com\Users		NT AUTHC	0	Yes	Read	Everyone	S-1-1-0	Allow	#########	0	

PowerHuntShares

- Installation
- Execution
- Reporting

Report



```
PS C:\temp> $MyShares = import-csv acme.local-Shares-Inventory-Excessive-Privileges.csv
PS C:\temp> $MyShares | Select -First 1


ComputerName       : Computer 1.acme.com
IpAddress          : 10.2.75.70
ShareName          : Monitor
SharePath          : \\computer1.acme.com.acme.local\Monitor
ShareDescription   : Dell EqualLogic SAN Headquarters logs
ShareOwner         : BUILTIN\Administrators
ShareType          : 0
ShareAccess        : Yes
FileSystemRights   : Read
IdentityReference  : BUILTIN\Users
IdentitySID        : S-1-5-32-545
AccessControlType  : Allow
LastModifiedDate   : 1/13/2022 16:46
FileCount          : 80
FileList           : Auto-Pilot
                     CredCache
                     FailedImport
                     Inbox
                     Queries
                     Traces
```

PowerHuntShares

- Overview
- Installation
- Execution
- Reporting

Demo Time!

```
PS C:\Users\player2>
```

Questions?

slides will be shared on twitter

@_nullbind

Always-on Pentesting

Platform Driven, Human Delivered.

WWW.NETSPI.COM | SALES@NETSPI.COM

NETSPI™

NETSPI™

WE’RE GROWING!

JOIN US!

See current openings: www.netspi.com/careers

Send us your resume: jobs@netspi.com

NetSPI Benefits

- ✓ Flexible time off
- ✓ Competitive pay
- ✓ Medical, dental, vision, & disability insurance
- ✓ HSA match
- ✓ 401k match
- ✓ Office perks: parking, game room, networking opportunities, Friday lunches