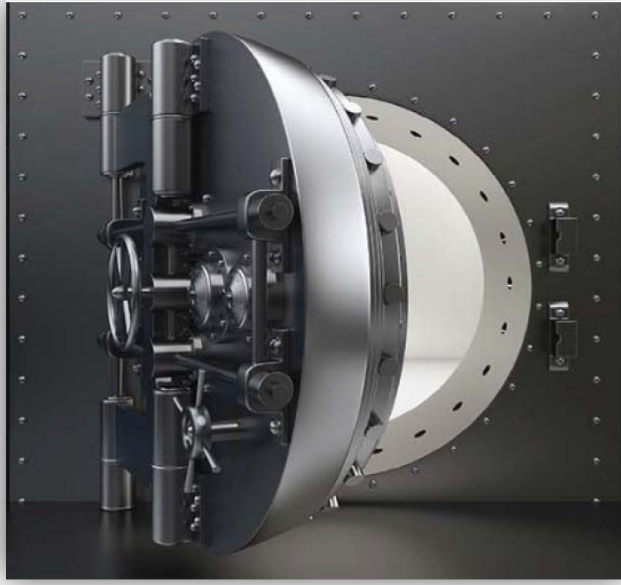




# Secure Guard Consulting

Secure Guard Consulting | (515) 229-5674 | [kkothari@sgcsecure.com](mailto:kkothari@sgcsecure.com) | [www.secureguardconsulting.com](http://www.secureguardconsulting.com)

**Secure Guard Consulting LLC** - [www.secureguardconsulting.com](http://www.secureguardconsulting.com)



Secure Guard Consulting performs full-service cybersecurity/IT auditing and consulting. This includes internal security assessments, external security assessments and external penetration testing, IT general controls reviews, and social engineering (phishing, phone, in-person). The company was founded in 2012 by Kaushal Kothari, a certified ethical hacker and former FDIC IT examination analyst.

**CONTACT:**

Kaushal Kothari  
Secure Guard Consulting  
180 Aidan Street, Waukee IA 50263  
Phone: 515-229-5674 / Email: [kkothari@sgcsecure.com](mailto:kkothari@sgcsecure.com)

# ABOUT SECURE GUARD CONSULTING



# SGC WEBINARS

- If interested – go out to our website, [secureguardconsulting.com](http://secureguardconsulting.com) to look and see upcoming webinars.
- These are all slated for an hour, but I will only go as long as needed to get information across.
- Please let me know if there's an additional topic any of you would like to see covered, and if interested, continue to check on our website as we post new webinars.



# TODAY – AD AUDIT

- A set of PowerShell scripts to perform some AD Audit functions.
- Originally, we thought about running these as a separate audit, but realized quickly that this is really something that should be run more often than annually.
- So, we're releasing these for free.
- Thank you to all of the banks that helped us with testing these scripts.



# AD AUDIT

- First time running this can be overwhelming.
  - Brings in lots of information and accounts most banks don't know are out there.
- Common areas
  - Mailbox accounts
  - Service accounts
- For everything identified that sticks around and isn't disabled, we recommend populating the description field for the account, so every time you run this, the information is just there.
- We recommend running this quarterly to stay on top of things.
- NOTE: You will need admin, preferably domain admin capability to run these.



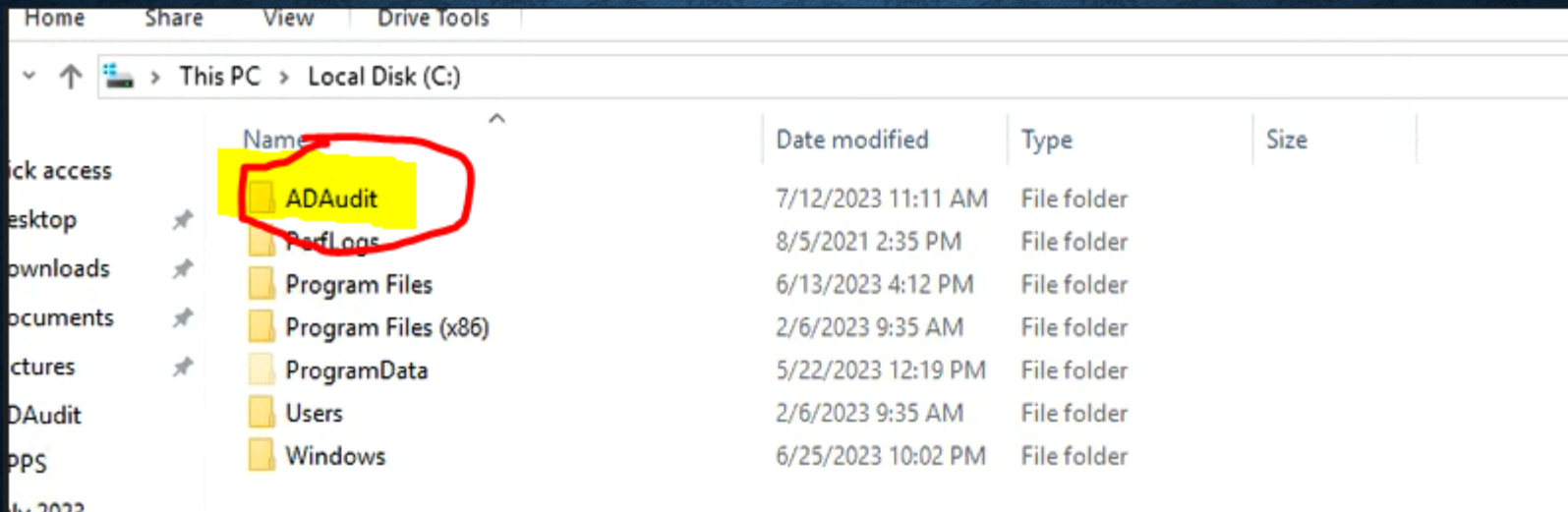
# **AD AUDIT INSTRUCTIONS**

(515) 229-5674 [kkothari@sgcsecure.com](mailto:kkothari@sgcsecure.com)



# AD AUDIT CORE

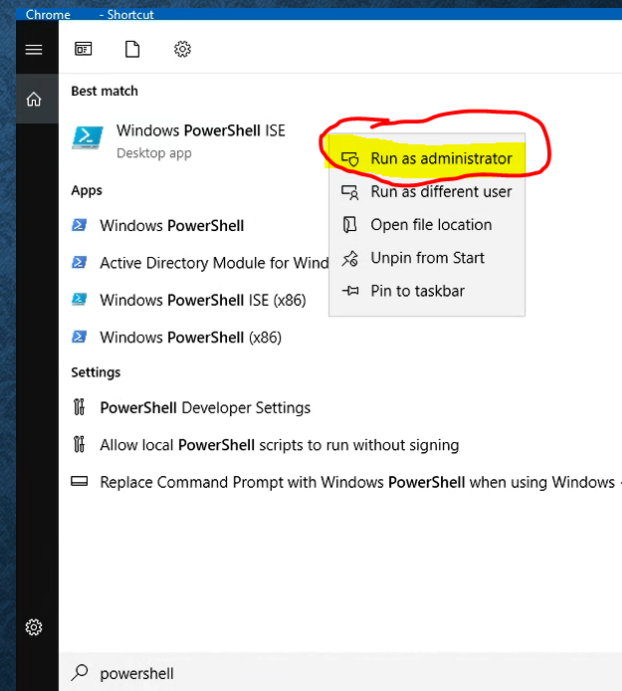
- Set up a folder in your C: drive (on the domain controller) called ADAudit (not case sensitive, but why take a chance 😊)





# AD AUDIT CORE

- Search for PowerShell and run Windows PowerShell ISE
- Right Click and Run as admin





# AD AUDIT CORE

- Move the three text files with the PowerShell code to your Domain Controller, or in a folder you can access from the Domain Controller.
  - ADAuditCore\_v10.txt
  - ADAuditMemberGroupsFinalNoBlankGroups\_v8.txt
  - ADAuditBlankGroupsFinal\_v1.txt



# AD AUDIT CORE

- Pull open code from “ADAuditCore\_v10.txt”
  - Select All
  - Copy
- Go to PowerShell and click in the window.
- Right click and Paste (or ctrl-V)
- Then hit Enter



# AD AUDIT CORE

- Disclaimer comes up. Click Enter to continue.

```
-----  
Welcome to Secure Guard Consulting Auditing Tool  
-----  
-----
```

## DISCLAIMER

```
-----  
This script is designed to perform an audit of your Active Directory system. It will ONLY collect  
emissions to run this script.
```

```
By continuing with the execution of this script, you acknowledge that Secure Guard Consulting and  
ript.
```

```
Press Enter to continue or Ctrl+C to exit.
```



# AD AUDIT CORE

- Prompt for either a custom path or the default path (C:\ADAudit).
  - I suggest just creating the right folder in the C Drive and clicking Enter.

Enter for default path. If choosing the default path, ensure a folder is created on the C: drive called





















# AD AUDIT CORE

- Once completed, you'll see a screen like below

```
Data export successful! The results were saved to C:\ADAudit.  
PS C:\Windows\system32> |
```



PC > Local Disk (C:) > ADAudit

Name	Date modified	Type	Size
 A. ADAuditSummary.csv	7/12/2023 11:17 AM	CSV File	1 KB
 B. PolicyInfo.csv	7/12/2023 11:17 AM	CSV File	1 KB
 C. EnabledAccounts.csv	7/12/2023 11:17 AM	CSV File	6 KB
 D. DisabledAccounts.csv	7/12/2023 11:17 AM	CSV File	1 KB
 E. Dormant 365 Days Plus.csv	7/12/2023 11:17 AM	CSV File	1 KB
 F. Dormant 90 to 365 Days.csv	7/12/2023 11:17 AM	CSV File	1 KB
 G. Dormant 45 to 90 Days NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
 H. NeverLoggedOn.csv	7/12/2023 11:17 AM	CSV File	1 KB
 I. PrivilegedUsers.csv	7/12/2023 11:17 AM	CSV File	1 KB
 J. PasswordNeverExpires.csv	7/12/2023 11:17 AM	CSV File	2 KB
 K. PasswordNotRequired NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
 L. SIDHistory NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
 M. ReversibleEncryption NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
 N. DESEncryption NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
 O. WithoutKerberosPreAuth NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
 P. ComputerAccounts.csv	7/12/2023 11:17 AM	CSV File	4 KB
 Q. ServerAccounts NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
 R. DCAccounts.csv	7/12/2023 11:17 AM	CSV File	1 KB



# AD AUDIT GROUPS AND MEMBERS

- Now do the same thing with the other code in  
“ADAuditMemberGroupsFinalNoBlankGroups\_v8.txt”
  - Open the text document, select all, copy, go to PowerShell, paste, click Enter
  - This second one there aren't any prompts, it just runs.



# AD AUDIT GROUPS AND MEMBERS

- Note: The script will error out on any groups that are set up as Foreign Security Principals (FSPs).
  - When a group from a trusted, external domain or forest is added to a group in the local domain, an FSP object is created in the local domain to represent the external group. This allows the local domain to recognize and work with the group from the external domain.
- Errors for FSPs will occur; these will be ignored; others will continue.
- IIS\_IUSRS Group is ignored by this script.



C:\ > Local Disk (C:) > ADAudit

Name	Date modified	Type	Size
A. ADAuditSummary.csv	7/12/2023 11:17 AM	CSV File	1 KB
B. PolicyInfo.csv	7/12/2023 11:17 AM	CSV File	1 KB
C. EnabledAccounts.csv	7/12/2023 11:17 AM	CSV File	6 KB
D. DisabledAccounts.csv	7/12/2023 11:17 AM	CSV File	1 KB
E. Dormant 365 Days Plus.csv	7/12/2023 11:17 AM	CSV File	1 KB
F. Dormant 90 to 365 Days.csv	7/12/2023 11:17 AM	CSV File	1 KB
G. Dormant 45 to 90 Days NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
H. NeverLoggedOn.csv	7/12/2023 11:17 AM	CSV File	1 KB
I. PrivilegedUsers.csv	7/12/2023 11:17 AM	CSV File	1 KB
J. PasswordNeverExpires.csv	7/12/2023 11:17 AM	CSV File	2 KB
K. PasswordNotRequired NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
L. SIDHistory NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
M. ReversibleEncryption NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
N. DESEncryption NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
O. WithoutKerberosPreAuth NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
P. ComputerAccounts.csv	7/12/2023 11:17 AM	CSV File	4 KB
Q. ServerAccounts NoData.csv	7/12/2023 11:17 AM	CSV File	0 KB
R. DCAccounts.csv	7/12/2023 11:17 AM	CSV File	1 KB
S. ADGroupsAndMembers.csv	7/12/2023 11:19 AM	CSV File	10 KB



# AD AUDIT BLANK GROUPS

- Now do the same thing again with the other code in “ADAuditBlankGroupsFinal\_v1.txt”
  - Open the text document, select all, copy, go to PowerShell, paste, click Enter
  - This third one there aren't any prompts, it just runs.
  - Errors for FSPs will also occur here, but those with FSPs will just be ignored. Those without will continue.



Local Disk (C:) > ADAudit

Name	Date modified	Type	Size
A. ADAuditSummary.csv	7/19/2023 9:05 PM	Microsoft Excel Com...	1 KB
B. PolicyInfo.csv	7/19/2023 9:07 PM	Microsoft Excel Com...	1 KB
C. EnabledAccounts.csv	7/19/2023 9:44 PM	Microsoft Excel Com...	1 KB
D. DisabledAccounts.csv	7/19/2023 9:45 PM	Microsoft Excel Com...	1 KB
E. Dormant 365 Days Plus.csv	7/19/2023 9:47 PM	Microsoft Excel Com...	1 KB
F. Dormant 90 to 365 Days.csv	7/19/2023 9:48 PM	Microsoft Excel Com...	1 KB
G. Dormant 45 to 90 Days NoData.csv	7/19/2023 9:03 PM	Microsoft Excel Com...	0 KB
H. NeverLoggedOn.csv	7/19/2023 9:49 PM	Microsoft Excel Com...	1 KB
I. PrivilegedUsers.csv	7/19/2023 9:53 PM	Microsoft Excel Com...	1 KB
J. PasswordNeverExpires.csv	7/19/2023 9:54 PM	Microsoft Excel Com...	1 KB
K. PasswordNotRequired.csv	7/19/2023 9:55 PM	Microsoft Excel Com...	1 KB
L. SIDHistory NoData.csv	7/19/2023 9:03 PM	Microsoft Excel Com...	0 KB
M. ReversibleEncryption NoData.csv	7/19/2023 9:03 PM	Microsoft Excel Com...	0 KB
N. DESEncryption.csv	7/19/2023 9:55 PM	Microsoft Excel Com...	1 KB
O. WithoutKerberosPreAuth NoData.csv	7/19/2023 9:03 PM	Microsoft Excel Com...	0 KB
P. ComputerAccounts.csv	7/19/2023 9:56 PM	Microsoft Excel Com...	1 KB
Q. ServerAccounts NoData.csv	7/19/2023 9:03 PM	Microsoft Excel Com...	0 KB
R. DCAccounts.csv	7/19/2023 10:00 PM	Microsoft Excel Com...	1 KB
S. ADGroupsAndMembers.csv	7/19/2023 10:02 PM	Microsoft Excel Com...	1 KB
T. BlankADGroups.csv	7/20/2023 12:08 AM	Microsoft Excel Com...	1 KB



# **AD AUDIT REFERENCE**

(515) 229-5674 [kkothari@sgcsecure.com](mailto:kkothari@sgcsecure.com)



# AD AUDIT REFERENCE

- Total Users
- Enabled Users
- Disabled Users
- Dormant accounts: Accounts that haven't been logged into
  - Between 45 and 90 days (CIS Controls driven)
  - Between 90 and 365 days
  - Greater than 365 days (Focus on this to start with!)



# AD AUDIT REFERENCE

- Accounts that have Never Logged On
  - Why do these accounts exist if they haven't been used?
- Privileged Users
- Computer Accounts (this we just added for informational)
- Server Accounts (same as Computer Accounts): Often times, servers are designated as Computer Accounts, so this may or may not be populated.
- DC Accounts



# AD AUDIT REFERENCE

- Accounts where the Password Never Expires.
  - Generally, these will be service accounts.
  - It's important to know and make sure though.
- Accounts with Password Not Required.
  - Although a password may exist, a password should be required.



- Accounts with SID History
- The Security Identifier (SID) is a unique value that is used to identify an object, such as a user or a group, in the Windows security system.
- Every object has a unique SID that is issued by Windows when the object is created, and this SID becomes part of the access token for that object.
  - The access token, in turn, is used by Windows whenever that object (or a process running as that object) attempts to access a secured resource.
- SID History is an attribute in Active Directory used to store former SIDs used by a user account. It comes into play when migrating accounts from one domain to another.
- When you move a user account between domains (e.g., during domain consolidation or migration), a new SID is created for the user account in the new domain. To allow for seamless resource access, the old SID is added to the SID History attribute of the user account in the new domain.
- This is useful because any permissions or rights that were assigned using the old SID will continue to work even after the account has been moved to the new domain. The Windows security subsystem checks both the account's current SID and the SIDs in the SID History attribute when determining the user's access rights.
- While useful, the SID History attribute can also pose a security risk if not properly managed. Old SIDs can potentially be used to gain unauthorized access, so it's generally recommended to clear the SID History once the domain migration is complete and all resources have been properly re-permissioned using the new SIDs.



# AD AUDIT REFERENCE

- Accounts with Reversible Encryption
  - The option to store passwords using reversible encryption provides support for applications that require the user's password for authentication. Anyone who knows the account password can misuse the account. Microsoft recommends disabling this setting through Group Policy
- Accounts with DES Encryption
  - Accounts that can use DES to authenticate to services are at significantly greater risk of having that account's logon sequence decrypted and the account compromised, since DES is considered weaker cryptography.



# AD AUDIT REFERENCE

- Accounts without Kerberos Pre Auth
  - Kerberos preauthentication is a process where the client's identity is verified before any Kerberos tickets are issued.
  - When the "Do not require Kerberos preauthentication" option is enabled for an account, it means this preauthentication step is skipped, and any client can request a Ticket Granting Ticket (TGT) for the user without needing to provide the proof of identity.
  - users who have the "Do not require Kerberos preauthentication" option set (enabled)



# AD AUDIT REFERENCE

- Account lockout threshold, password complexity enabled, lockout duration, password expiration, etc.
- KRBtgt Account
  - The KRBtgt account is a domain default account that acts as a service account for the KDC service. In most cases, KRBtgt resets might be performed when Active Directory is compromised. Still, Microsoft advises changing the password at regular intervals to keep the environment more secure.
  - Either Disable or change password every 180 days.
    - If changing password, needs to be changed twice in quick succession – make sure to consult your MSP for this.



# AD AUDIT REFERENCE

- Tombstone Policy number of days
  - The tombstone lifetime in Active Directory refers to the period of time that a deleted object (such as a user or computer account) is retained in the Active Directory database before it is permanently deleted. This period of time is also referred to as the deleted object's "tombstone lifetime."
  - When an object is deleted from Active Directory, it isn't immediately removed from the database. Instead, most of the object's attributes are cleared out, and the object is marked as a "tombstone" and moved to a special container called the Deleted Objects container. The object will then remain in this state for the duration of the tombstone lifetime.
  - If blank, defaults are used (60 or 180). Microsoft recommends 180 days. Check to make sure your default is 180 days, or set it to 180 days.



# AD AUDIT REFERENCE

Forest Functional Level of the Domain Controller	Tombstone lifetime in days
Windows Server 2012	180
Windows Server 2008 R2	180
Windows Server 2008	180
Windows Server 2003 R2 SP2	180
Windows Server 2003 R2 SP1	60
Windows Server 2003 R2	60
Windows Server 2003 SP2	180
Windows Server 2003 SP1	180
Windows Server 2003 RTM	60



# AD GROUP MEMBERSHIP AUDIT REFERENCE

- AD Groups and Members – Internal AD Review
  - Look through and make sure each group's members should actually be members of each group.



# AD BLANK GROUP AUDIT REFERENCE

- AD Blank Groups (No Members) – Internal AD Review
  - Look through and make sure each blank group to see whether it is needed any longer, especially since it doesn't have any members.