📄 Identity and Access Management (IAM) Lab Report

Zakiya Moore

Table of Contents

---

1. Introduction

This lab demonstrates the implementation of basic Identity and Access Management (IAM) principles in a Windows 11 environment.
The objective was to create users, define groups, assign permissions based on least privilege, automate folder access controls, and validate all settings using PowerShell scripting.
All tasks were performed in a virtualized environment with professional-level documentation and automation.

---

2. Environment Setup

The lab was completed inside a Windows 11 Virtual Machine hosted on VirtualBox.
To address disk space constraints, a Shared Folder was used to store all scripts, screenshots, and reports.

IAM_Lab Folder Structure:

CopyEdit

```
IAM_Lab/
 ├── Users_Scripts/
 ├── Groups_Scripts/
 ├── AddToGroups_Scripts/
 ├── Folder_Permissions/
 ├── Screenshots/
 ├── Validation_Check.ps1
```

Scripts were created and executed from the Shared Folder mapped as drive Z: inside the VM.

---

3. User Creation

Three users were created using a PowerShell script (Create_Users.ps1):

- analyst_user1 — Security Analyst
- admin_user2 — IT Administrator
- intern_user3 — Intern

Validation:

```
Administrator: Windows PowerShell
PS C:\IAM_Lab> cd C:\IAM_Lab\
PS C:\IAM_Lab> dir


    Directory: C:\IAM_Lab


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/25/2025   9:21 PM                AddToGroups_Scripts
d-----         4/25/2025   9:31 PM                Folder_Permissions
d-----         4/25/2025   9:20 PM                Groups_Scripts
d-----         4/25/2025   9:30 PM                Screenshots
d-----         4/25/2025   9:19 PM                Users_Scripts


PS C:\IAM_Lab>
```

Figure 1: User accounts created via Create_Users.ps1

---

4. Group Creation and Membership Validation

Two security groups were created to enforce role-based access control policies:

- Security_Analysts
- IT_Administrators

Group creation was validated using the Get-LocalGroup command.

```
PS Z:\IAM_Lab> Get-LocalGroup

Name                                Description
----                                -----------
IT_Administrators                   Full control over admin tools
Security_Analysts                   Read access to security logs
Access Control Assistance Operators Members of this group can remotely query...
Administrators                      Administrators have complete and unrestr...
Backup Operators                    Backup Operators can override security r...
Cryptographic Operators             Members are authorized to perform crypto...
Device Owners                       Members of this group can change system-...
Distributed COM Users               Members are allowed to launch, activate ...
Event Log Readers                   Members of this group can read event log...
Guests                              Guests have the same access as members o...
Hyper-V Administrators              Members of this group have complete and ...
IIS_IUSRS                           Built-in group used by Internet Informat...
Network Configuration Operators     Members in this group can have some admi...
OpenSSH Users                       Members of this group may connect to thi...
Performance Log Users               Members of this group may schedule loggi...
Performance Monitor Users           Members of this group can access perform...
Power Users                         Power Users are included for backwards c...
Remote Desktop Users                Members in this group are granted the ri...
Remote Management Users             Members of this group can access WMI res...
Replicator                          Supports file replication in a domain
System Managed Accounts Group       Members of this group are managed by the...
User Mode Hardware Operators        Members of this group may operate hardwa...
Users                               Users are prevented from making accident...


PS Z:\IAM_Lab>
```

Figure 2: Local groups created via Create_Groups.ps1.

After group creation, users were assigned to appropriate groups to follow the principle of least privilege:

- analyst_user1 and intern_user3 were assigned to Security_Analysts.
- admin_user2 was assigned to IT_Administrators.

Group memberships were validated using the Get-LocalGroupMember command.

```
Administrator: Windows PowerShell
PS Z:\IAM_Lab> Get-LocalGroupMember -Group "Security_Analysts"
>>

ObjectClass Name                 PrincipalSource
----------- ----                 ---------------
User        Zakiya\analyst_user1 Local
User        Zakiya\intern_user3  Local


PS Z:\IAM_Lab> Get-LocalGroupMember -Group "IT_Administrators"

ObjectClass Name               PrincipalSource
----------- ----               ---------------
User        Zakiya\admin_user2 Local
```

Figure 3: Group memberships validated via Get-LocalGroupMember command.

---

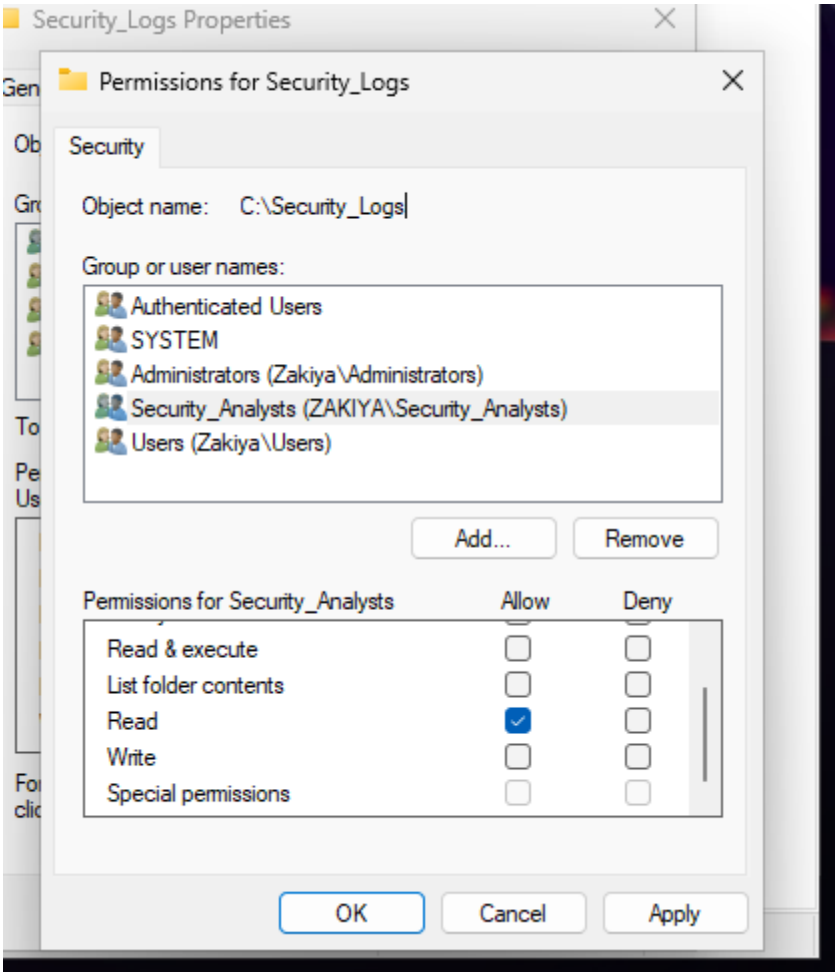
5. Folder and Permissions Setup

Two folders were created:

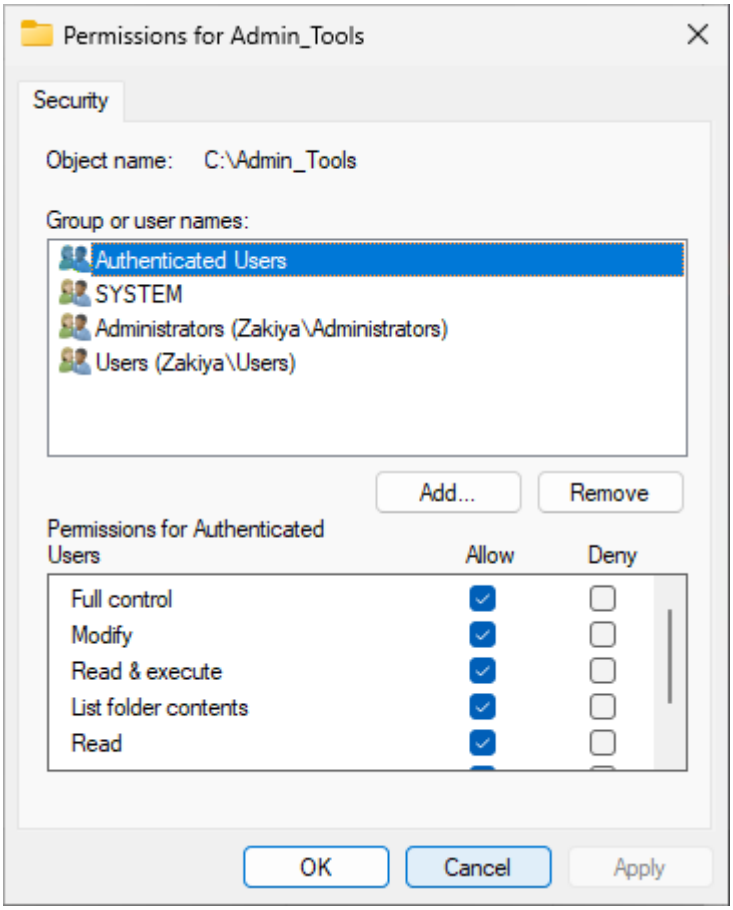
Folder	Group Access	Permission
Security_Logs	Security_Analysts	Read-only
Admin_Tools	IT_Administrators	Full Control

Permissions were applied using the Folder_Permissions.ps1 script.

Validation:



Security_Logs_Permissions.png



Admin_Tools_Permissions.png

---

6. Validation and Testing

The Validation_Check.ps1 script was used to verify:

- All users exist
- All groups exist
- Users are assigned correctly to groups

Validation:

CR

```
Administrator: Windows PowerShell
Event Log Readers                    Members of this group can read event log...
Guests                               Guests have the same access as members o...
Hyper-V Administrators               Members of this group have complete and ...
IIS_IUSRS                            Built-in group used by Internet Informat...
Network Configuration Operators      Members in this group can have some admi...
OpenSSH Users                        Members of this group may connect to thi...
Performance Log Users                Members of this group may schedule loggi...
Performance Monitor Users            Members of this group can access perform...
Power Users                          Power Users are included for backwards c...
Remote Desktop Users                 Members in this group are granted the ri...
Remote Management Users              Members of this group can access WMI res...
Replicator                           Supports file replication in a domain
System Managed Accounts Group        Members of this group are managed by the...
User Mode Hardware Operators         Members of this group may operate hardwa...
Users                                Users are prevented from making accident...


==== Checking Group Memberships ====

Security_Analysts Members:

Name                 ObjectClass
----                 -----------
Zakiya\analyst_user1 User
Zakiya\intern_user3  User


IT_Administrators Members:

Name                ObjectClass
----                -----------
Zakiya\admin_user2 User


==== Validation Complete! ====
PS Z:\IAM_Lab>
```

Figure 6: Validation of users, groups, and group memberships

Additionally, login tests were performed:

- Analysts could read but not modify files in Security_Logs.
- Admins could fully control Admin_Tools.

---

7. Challenges Encountered

- Disk space inside the VM was insufficient, causing storage errors.
- Shared Folders were configured in VirtualBox to move the project onto the host machine safely.
- Execution policies in PowerShell needed to be bypassed to allow script execution.

---

8. Lessons Learned

- Importance of clean environment setup and folder organization.
- PowerShell scripting can fully automate IAM tasks in Windows.
- Validation and documentation are critical for cybersecurity projects.
- Shared Folders are an effective workaround for VM storage limitations.

---

19. Conclusion

This IAM Lab successfully demonstrated the ability to automate and validate fundamental identity and access management tasks in a secure Windows environment.
Scripting users, groups, permissions, and verifying security settings prepares the foundation for larger enterprise IAM operations.
This hands-on experience reinforced cybersecurity best practices and documentation standards for real-world defensive security work.