SECURITY WALKTHROUGH

Active Directory Basics

Submitted to: << sprints >>

Security Analyst: << team4 >>

Team Members :

- **Security Analyst: << Ali Mohamed Abdelfatah >>**
- **Security Analyst: << Mohamed Ahmed Fathy>>**
- **Security Analyst: << Tarek Ayman Hassan>>**
- **Security Analyst: << Ali Samy Gomaa>>**
- **Security Analyst: << Zyad Mohamed Hagag>>**

1. Introduction

This report focuses on the findings from an Active Directory (AD) assessment, which includes understanding the core structure and functioning of a Windows domain, its vulnerabilities, and how certain elements in AD can be exploited or configured for better security. The objective of this penetration test was to assess potential security gaps in AD and provide actionable recommendations for improvement.

2. Active Directory Overview

Active Directory is a centralized database that stores information about objects such as users, computers, and other resources within the network. It allows for streamlined management of domain resources. Windows Domains utilize AD to manage large sets of users and computers.

2.1 Active Directory Components

- **Active Directory:** The centralized repository for storing user credentials and other domain-related information.
- **Domain Controller (DC):** The server responsible for running Active Directory services.
- **Users, Machines, and Groups:**
  - **Users** represent people with domain access.
  - **Machines** are computers added to the domain.
  - **Groups** (e.g., **Domain Admins**) manage computers and resources across the domain.

3. Task-Based Assessment

Task 2: **Basic Active Directory Queries**

1. **Where are credentials stored in a Windows domain?**
    - **Answer:** Active Directory
2. **What is the server responsible for running Active Directory services?**
    - **Answer:** Domain Controller

Task 3: **Active Directory User Management**

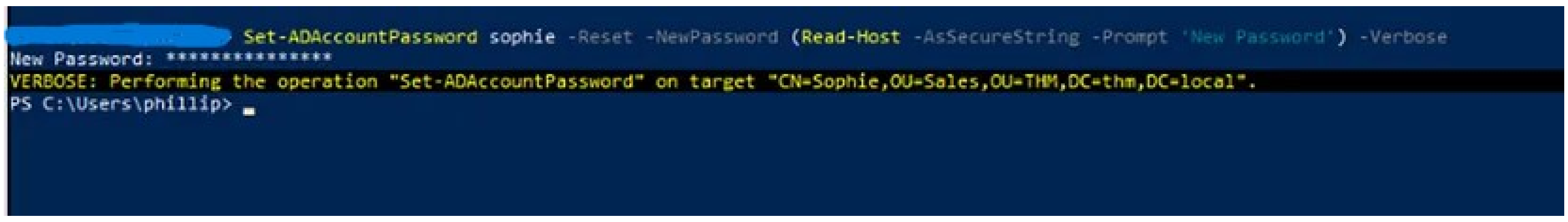
1. **Which group manages all computers and resources in the domain?**
    - **Answer:** Domain Admins
2. **What is the machine account name for a computer called TOM-PC?**
    - **Answer:** TOM-PC$
3. **What container should we use for organizing users in the Quality Assurance department?**
    - **Answer:** Organizational Units

Task 4: **User Privileges and Delegation**

1. **What was the flag found on Sophie's desktop?**

    - **Answer:** THM{thanks_for_contacting_support}

    Procedure:

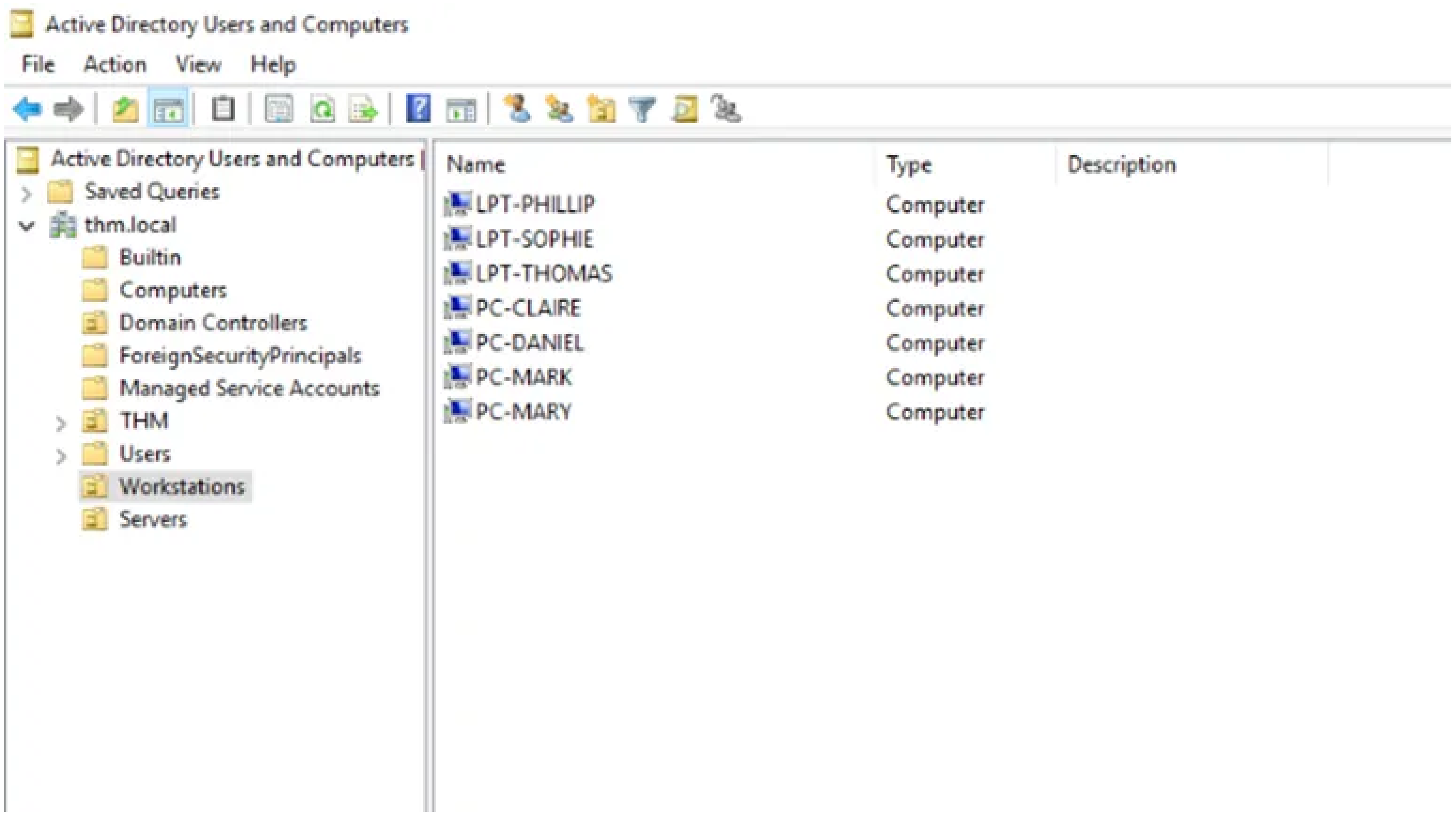
    - Access was granted via Remote Desktop Protocol (RDP), and the password reset procedure was executed through PowerShell after elevating privileges using Phillip's account. Once logged in as Sophie, the flag was retrieved.
    - 

```
[redacted] Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose
New Password: ***************
VERBOSE: Performing the operation "Set-ADAccountPassword" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip> _
```

2. **What is the process of granting privileges over an AD Object called?**
    - **Answer:** Delegation

Task 5: **Managing Computers in Active Directory**

1. **How many computers were moved to the Workstations OU?**
    - **Answer:** 7

- 

Name	Type	Description
LPT-PHILLIP	Computer	
LPT-SOPHIE	Computer	
LPT-THOMAS	Computer	
PC-CLAIRE	Computer	
PC-DANIEL	Computer	
PC-MARK	Computer	
PC-MARY	Computer	

2. **Is it recommended to create separate OUs for Servers and Workstations?**
    - **Answer:** yay

Task 6: **Group Policy Management**

1. **What is the network share used to distribute GPOs?**
    - **Answer:** SYSVOL
2. **Can a GPO be used to apply settings to both users and computers?**
    - **Answer:** yay

Task 7: **Authentication Protocols in Active Directory**

1. **Will NetNTLM be used as the default authentication protocol in recent Windows versions?**
    - **Answer:** nay
2. **What type of Kerberos ticket allows further requests for TGS (Ticket Granting Service)?**
    - **Answer:** Ticket Granting Ticket (TGT)
3. **Is a user's password transmitted over the network when using NetNTLM?**
    - **Answer:** nay

Task 8: **Active Directory Trees and Trusts**

1. **What is a group of Windows domains that share the same namespace called?**
    - **Answer:** Tree
2. **What should be configured between two domains for cross-domain resource access?**
    - **Answer:** Trust Relationship

4. Findings and Recommendations

Based on the Active Directory review, the following areas were highlighted for improvement:

4.1 User Management

- **Finding:** The current structure for users and groups seems to be well-organized, but there may be over-permissive accounts or dormant user accounts that need to be disabled or removed.
- **Recommendation:** Regular audits of users and permissions should be conducted, particularly in high-privilege groups such as Domain Admins.

4.2 Group Policy Security

- **Finding:** GPOs are appropriately managed through the SYSVOL share; however, if GPOs are not properly audited, there is potential for misconfiguration.
- **Recommendation:** Implement a stricter review process for GPOs to prevent accidental misconfigurations that could lead to security risks.

4.3 Authentication Protocols

- **Finding:** While Kerberos is the default protocol, the continued use of legacy protocols like NetNTLM poses a risk.
- **Recommendation:** Disable NetNTLM across the domain if possible, and enforce Kerberos for all authentication to mitigate the risk of credential relay attacks.

4.4 Trust Relationships

- **Finding:** Trust relationships between domains should be closely monitored, as improper configuration can lead to unauthorized access.
- **Recommendation:** Ensure that trust relationships are properly set up, with regular reviews of cross-domain permissions.