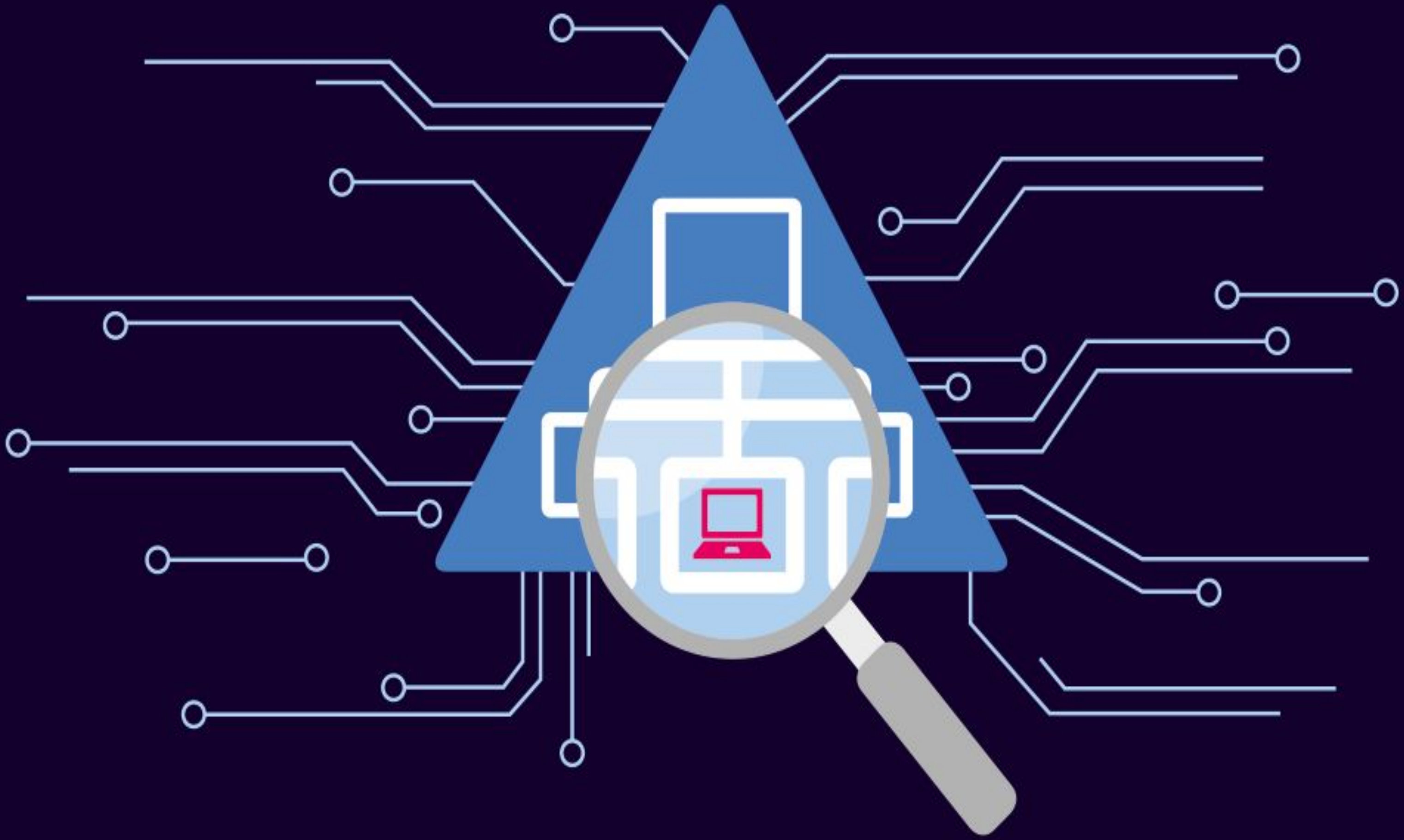
ACTIVE DIRECTORY SECURITY ASSESSMENT (ADSA)



Echo ‘Whoami’

- 3rd year Computer Engineering Student at NMIMS
- Interned with Deloitte in their Cyber Risk Department
- Currently volunteering as a TA at Cybrary involved in beta testing, quiz question creation and much more
- Interested in all things relating to cybersecurity
- Email - navidkagalwalla27@gmail.com

ACTIVE DIRECTORY - “THE KEYS TO THE KINGDOM”

WHAT IS COVERED

1. What is AD?
2. What is ADSA?
3. Why is ADSA required?
4. Phases of ADSA
5. Key Assessment Areas of ADSA
6. Key Benefits of ADSA
7. ADSA Checklist
8. Practical Report of ADSA

WHAT IS AD?

- Active Directory provides mission-critical
  - Authentication
  - Authorization
  - Configuration capabilities

  to manage users, computers, servers and applications throughout an organization’s IT infrastructure

- Primary system that attackers go after once they gain initial access into an environment. They scan and leverage Active Directory to perform reconnaissance, escalate privileges, access data and persist in the environment

WHAT IS ADSA?

- Helps an organization to identify, quantify and reduce the risks affecting the security of one of the most critical infrastructure components in most IT environments

- Includes both technical and non-technical fronts

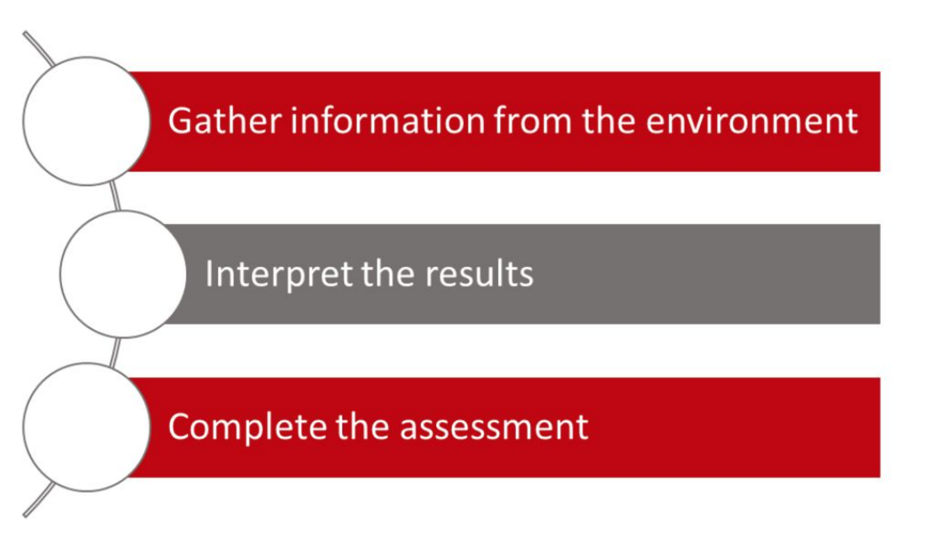
- Provides prioritized, structured remediation advice, allowing an organization to easily identify where efforts should be focused

WHY IS ADSA REQUIRED?

- Organizations’ implementations of Active Directory evolve
- Provides a holistic assessment of the security of an Active Directory installation
- Comprehensive analysis of both technical and non-technical risks
- Significant cost savings can be realized by leveraging prioritized, actionable guidance to secure existing investments rather than increasing cost and complexity by adding additional security components that may be unnecessary in the presence of a secure AD implementation.

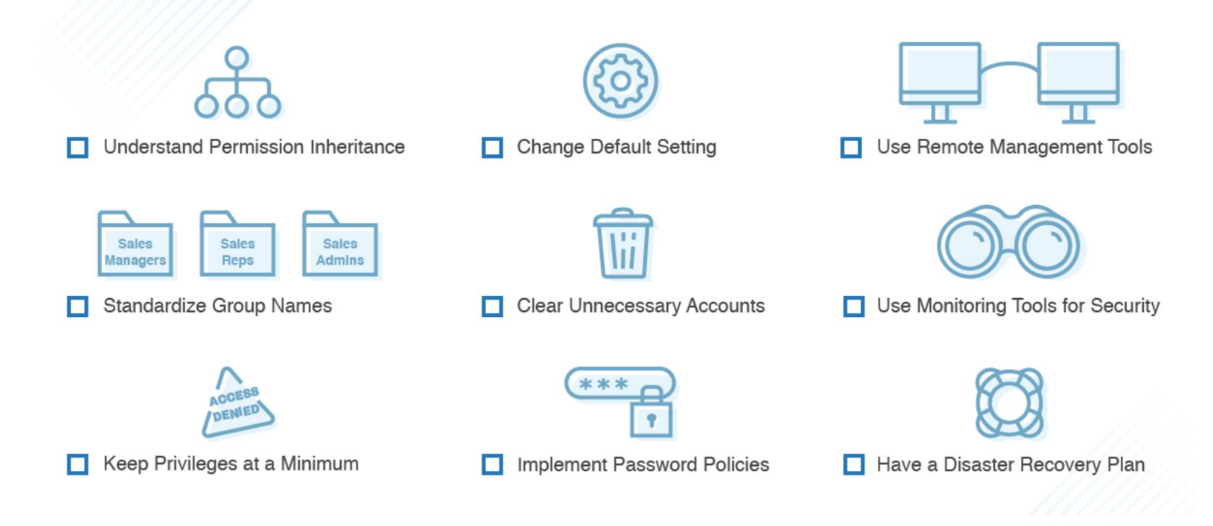
PHASES OF ADSA

- The Assessment Process has four primary phases :
  - Gather data from the environment, while on-site or remote
  - Interpret and analyze the results
  - Complete the assessment report
  - Provide detailed recommendations



KEY ASSESSMENT AREAS OF ADSA

- Configuration Visibility and Management
- Group Policy and Privilege Controls
- Recommendations and Plans



□ Understand Permission Inheritance

□ Standardize Group Names

□ Keep Privileges at a Minimum

□ Change Default Setting

□ Clear Unnecessary Accounts

□ Implement Password Policies

□ Use Remote Management Tools

□ Use Monitoring Tools for Security

□ Have a Disaster Recovery Plan

KEY BENEFITS OF ADSA

- Domain Controllers Security
- Administrative Memberships
- Operational Excellence
- Knowledge Transfer

ADSA CHECKLIST

- The logical (forest, domain and trust-relationship) structure of the Active Directory is secure
- Active Directory configuration (e.g. Schema, Replication, FSMOs, Backups) data is secure
- Active Directory management, security and disaster-recovery plans are in place and implemented
- Physical, system and network security is provided for all Domain Controllers and admin workstations
- Number of IT personnel who possess unrestricted administrative access in Active Directory is minimal
- All non-critical administrative tasks (e.g. password resets) are delegated based on the principle of least privilege
- IT personnel can audit all administrative delegations in Active Directory
- Auditing mechanisms are in place to capture the enactment of all admin/delegated tasks in Active Directory
- All applications and tools used by IT personnel are trustworthy
- Effective access audits are performed on a regular basis to consistently ensure security

PRACTICAL REPORT OF ADSA