1

IT Solution

IT 493-004 Alpha Team 4

CHRISTOPHER KYRIACOU | JAMIE SUTTON | NATHAN CHONG | **SAFEE GHAFOORI** | DAVE FULLER

2 Target Solution

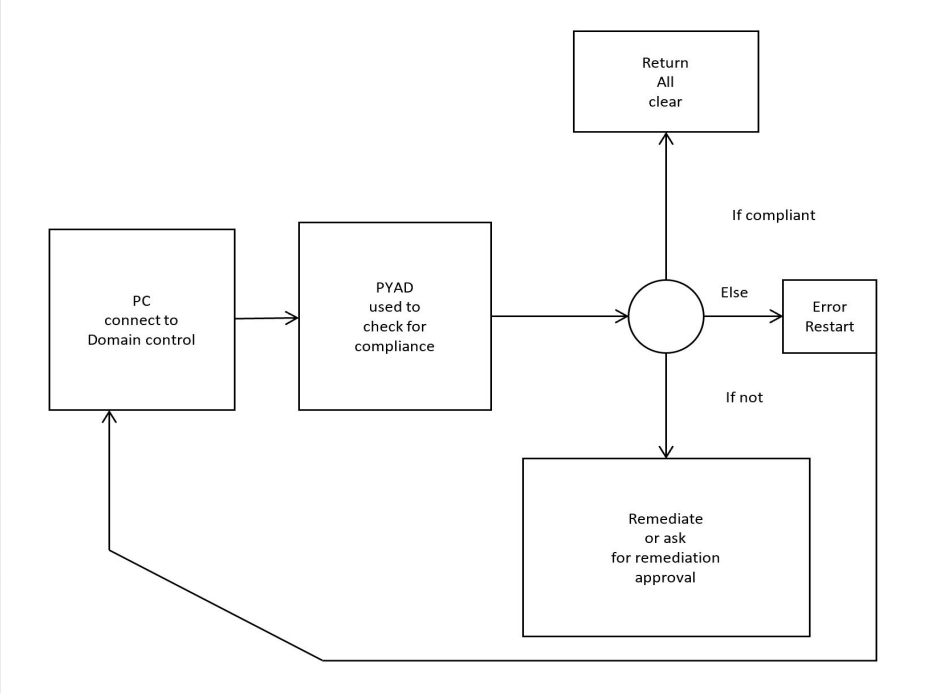
- **Our solution aims to create a secure auditing system that allows authorized security admin to audit their Active Directory (AD) servers for CMMC compliance**
- **Auditing system will entail:**
  1. Having a PC remotely connect to the Domain Controller
  2. Utilizing Python along with the Python AD (pyad) package to check for compliance
  3. Prompt the admin to perform remediation
  4. Generate a report with audit findings

3 Target Solution (cont.)

Functionality list to reach our main goal:

1. **Use AD to identify computers, verify that the computer has a distinct name, the name follows the convention, and it requires the user to log in**
2. **List the users and computers in AD who have not logged in in N days**
3. **Produce a list of users who have not changed their password in N days**
4. **Produce a list of users in a given AD section (i.e., restrict.xxx.com) who have administrative privileges**
5. **For service accounts, ensure that the "manager" field is filled out. A question is how to identify service accounts. There is a naming convention, but we do not know if it is followed (another audit requirement)**
6. **For all accounts, the "password expire" flag is set.**
7. **Monitor for what process is communicating with a given IP and/or port on the Active Directory Server from a remote host.**

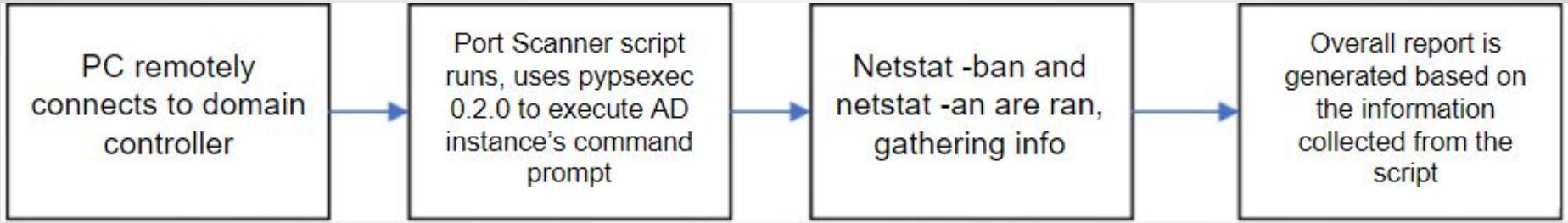
4 Logical Solution



5 Functional Solution

- **Bash script is initiated to securely pass credentials and variables then executes the Python script**
- **Using pyad, Python script attempts to retrieve all information requested from the AD server, with the ability for the admin to remediate**
- **A final report is generated with the requested information returned**

6 Functional Solution (cont.)



- **The Port_Scanner class tests the ability to run port scans on the socket level using socket and threading**
- **Used to run netstat -ban and netstat -an with Python PsExec Library (pypsexec) on the AD Server from a remote host**
- **Discovers what processes are connecting to active ports on the domain server itself as well as computers connected to the domain**

7 Solution Requirements

- Hardware:
  - Professional-grade laptop
  - Industry-grade server
- Software:
  - Must be able to run Python / all the Python packages used for the scripts
- Personnel:
  - At a minimum only one person (ARA Admin) is needed to execute the script, and it is up to the admin who to assign remediation to

8 Questions?