

# Security and Auditing of Active Directory

Pratik Solanki, Harpreet Kaur, Satvir Kaur

## Index

Chapter No.	Name	Page Number
1	Project Proposal	2
2	Literature Review	7
3	Methodology	15
4	Implementations and Results	22
5	Conclusion	29
6	References	31

# **1. Introduction**

## **A. Team Members**

1. Harpreet Kaur
2. Pratik Solanki
3. Satvir Kaur

## **B. Description**

- Most of the organizations store data on Active Working and there is very little security in enterprise when it comes to security for AD. Now in Conestoga the security of active directory is very important because anyone can still vulnerable data of students and faculties and use that for evil intentions.

## **2.Problem Statement**

**Objective:** The main objective of our project is to provide assurance that the data is secure. All the data of active directory is handled by Microsoft and security persons are overlooked so both developers and security people will have to come together to solve the security concerns regarding active directory.

**Scope:** The scope of this capstone project will consider the following modules.

- ❖ Active Directory management
- ❖ Secure Active Directory boundaries
- ❖ Secure domain controllers
- ❖ Physical security of the domain controllers
- ❖ Secure domain and domain controller configuration settings
- ❖ Secure administrative practices

## Threats to Active Directory

- Default Security Settings: Active directory has default settings for security by Microsoft. Hackers can understand default security very well and exploit vulnerabilities.
- Inappropriate Administrative Users and Privileged Access: Admins have full privileges or super user privileges without even need.
- Broad access for roles and employees: AD allows administrators to grant access to specific applications and data based on employee roles. Roles are assigned to groups that determine access levels. It's important to only allow the levels of access to individuals and roles need to perform their job functions.
- Simple passwords for admin accounts: Brute force attacks on AD services often target passwords. Uncomplicated passwords and easily guessable passwords are most at risk.
- Unpatched vulnerabilities on AD servers: Hackers can quickly exploit unpatched applications, OS, and firmware on AD Servers, giving them a critical first-foothold within your environment.
- Lack of visibility and reporting of unauthorized access attempts: If IT administrators have awareness about unauthorized access attempts, they can more effectively disrupt or prevent such access attempts in the future. Thus, a clear Windows audit trail is vital to identify both legitimate and malicious access attempts, and to detect any AD changes that have been made.

## **Best Practices for Active Directory Security**

There are at least 7 best practices IT departments should implement to ensure holistic security around Active Directory. These should at minimum include:

### **Review and Amend Default Security Settings**

After installing AD, it's vital to review the security configuration and update it in line with business needs.

### **Implement Principles of Least Privilege in AD Roles and Groups**

Review all the necessary permissions for data and applications for all employee roles in the organization. Ensure that employees have only the minimal level of access they need to perform their job roles. Also, ensure separation of privileges, so there is tighter auditability between roles and to help prevent lateral movement in the event an account is compromised. Apply strong privileged access management (PAM) policies and security controls.

### **Implement Robust AD Administration Privileges and Limit Domain User Accounts**

Carefully review all IT staff responsibilities and only provide administrative privileges and superuser access to those who absolutely need this access to perform their roles. Use PowerShell Just Enough Administration (JEA) and/or a PAM solution to ensure this access is limited in the most granular way practical. Ensure these accounts are properly protected with robust passwords.

### **Use Real-Time Windows Auditing and Alerting**

Conduct reporting of unusual access attempts. Provide full windows auditing and alerting of any access from inside or outside the organization. Pay special attention to Windows AD change auditing. This will also help to meet PCI, SOX, HIPAA, and other compliance requirements.

### **Ensure Active Backup and Recovery**

Backup the AD configuration and directory on a regular basis. Practice disaster recovery processes to allow for fast recovery in case AD integrity is breached.

### **Patch All Vulnerabilities Regularly**

Identifying and patching vulnerabilities is one of the IT department's most important tasks. Ensure a fast, efficient, effective patching and maintenance process for AD and other flaws.

#### Centralize and Automate

Centralize all reviews, reports, controls, and administration in one place, and look for tools that can provide automated workflows for alerting and helping to reconcile issues.

Understanding AD vulnerabilities and implementing security and least privilege access controls is vital to protecting domain accounts and keeping the IT ecosystem safe. Proper visibility, management, reporting, and auditing capabilities can significantly enhance AD security and ensure systems integrity.

## **Active Directory Security Assessment:**

It has total 3 phases

1. Gather data from environment
2. Interpret and analyze results
3. Complete assessment report and provide detailed recommendation

**A SECURE ACTIVE DIRECTORY ENVIRONMENT CAN MITIGATE MOST ATTACKS.**

### **3. Significance**

- We choose this project because the security of students information is very important and when the personal data is secure people will take admission without hesitation because attack on social data is one of the attack in current era and hackers use this information like to get bank password by providing personal data to customer service representative.

#### **4. Resources**

##### **A. Hardware**

1. Computer/Laptop with minimum of 8 GB RAM, Intel core processor i5 , 128 GB SSD , 2 GB Graphic Card

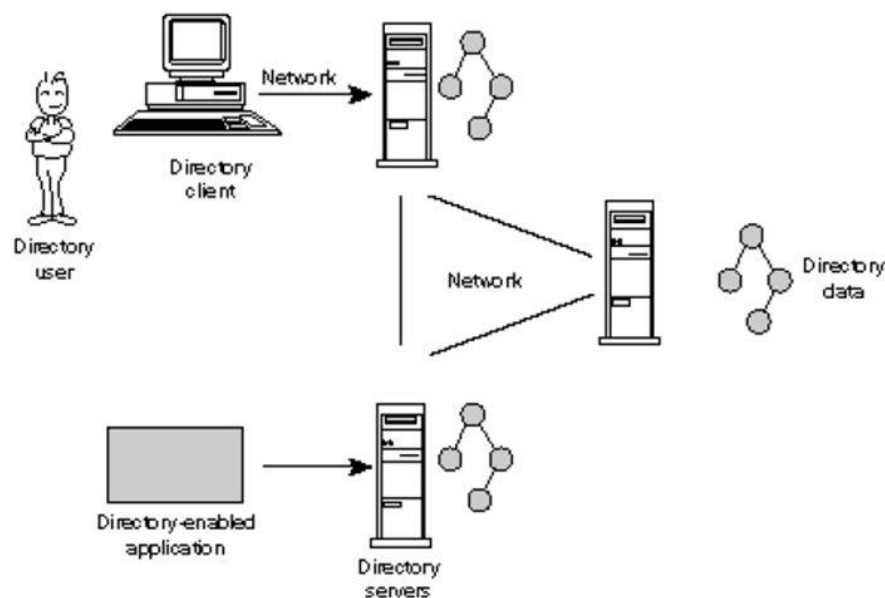
##### **B. Software**

1. LDAP Browser
2. Microsoft Visual Studio
3. Microsoft Visio
4. Microsoft Project
5. Microsoft Office 365

## Literature Review

A directory is a hierarchical structure that stores information about objects on the network. A directory service such as Active directory domain services, provides the methods for storing directory data and making data available to network users and administrators. For example, Active directory domain services stores information about user accounts, such as names, passwords, phone numbers and so on, and enables other authorized users on the same network to access this information (Flores, Billmath, Kumar, & Plett, 2017).

## Directory Service



3

Figure 1. Directory Services

Online directories are used by enterprises with distributed computer systems for fast searches, management of users and security, and integration of multiple applications and services. Online directories have become critical to e-businesses and hosted environments (Oracle, 2019).

## ROLE OF ONLINE DIRECTORIES

An online directory is a specialized database that stores and retrieves collections of information about objects. Such information can represent any resources that require management: employee names, titles, and security credentials; information about partners; or information about shared network resources such as conference rooms and printers (Oracle, 2019).

Online directories can be used by a variety of users and applications, and for a variety of purposes, including (Oracle, 2019): (Oracle, 2019)

- An employee searching for corporate white page information, and, through a mail client, looking up e-mail addresses
- An application, such as a message transport agent, locating a user's mail server
- A database application identifying role information for a user

Although an online directory is a database—that is, a structured collection of data- it is not a relational database. The following table contrasts online directories with relational databases (Oracle, 2019).

Online Directories	Relational Databases
Designed to handle relatively simple transactions on relatively small units of data. For example, an application might use a directory simply to store and retrieve an e-mail address, a telephone number, or a digital portrait (Oracle, 2019).	Designed to handle large and diverse transactions using many operations on large units of data (Oracle, 2019).
Designed to be location-independent. Directory-enabled applications expect, always, to see the same information throughout the deployment environment—regardless of which server they are querying. If a queried server does not store the information locally, then it must either retrieve the information or point the client application to it transparently (Oracle, 2019).	Typically designed to be location-specific. While a relational database can be distributed, it usually resides on a database server (Oracle, 2019).
Designed to store information in entries. These entries might represent any resource customers want to manage employees, e-commerce partners, conference rooms, or shared network resources such as printers. Associated with each entry are several attributes, each of which may have one or more values assigned. For example, typical attributes for a person entry might include first and last names, e-mail addresses, the	Designed to store information as rows in relational tables (Oracle, 2019).



address of a preferred mail server, passwords or other login credentials, or a digitized portrait (Oracle, 2019).	
---	--

## Language used in Active Directory

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a general-purpose data store and can be used in a wide variety of applications (LDAP.com, 2019).

LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for directory services in a network. LDAP is lighter because in its initial version it did not include security features (Rouse, 2019).

In a network, a directory tells you where in the network something is located. On TCP/IP networks, the domain name system is the directory system used to relate the domain name to a specific network address (Rouse, 2019). LDAP allows you to search for an individual without knowing where they're located (Rouse, 2019).

An LDAP directory is organized in a simple "tree" hierarchy consisting of the following levels (Rouse, 2019):

1. The root directory (the starting place or the source of the tree), which branches out to.
2. Countries, each of which branches out to.
3. Organizations, which branch out to.
4. Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for).
5. Organizational units (divisions, departments, and so forth), which branches out to (includes an entry for)

## LDAP Authentication

There are two options for LDAP authentication in LDAP v3 – simple and SASL (Simple Authentication and Security Layer) (Sobers, 2018).

Simple authentication allows for three possible authentication mechanisms:

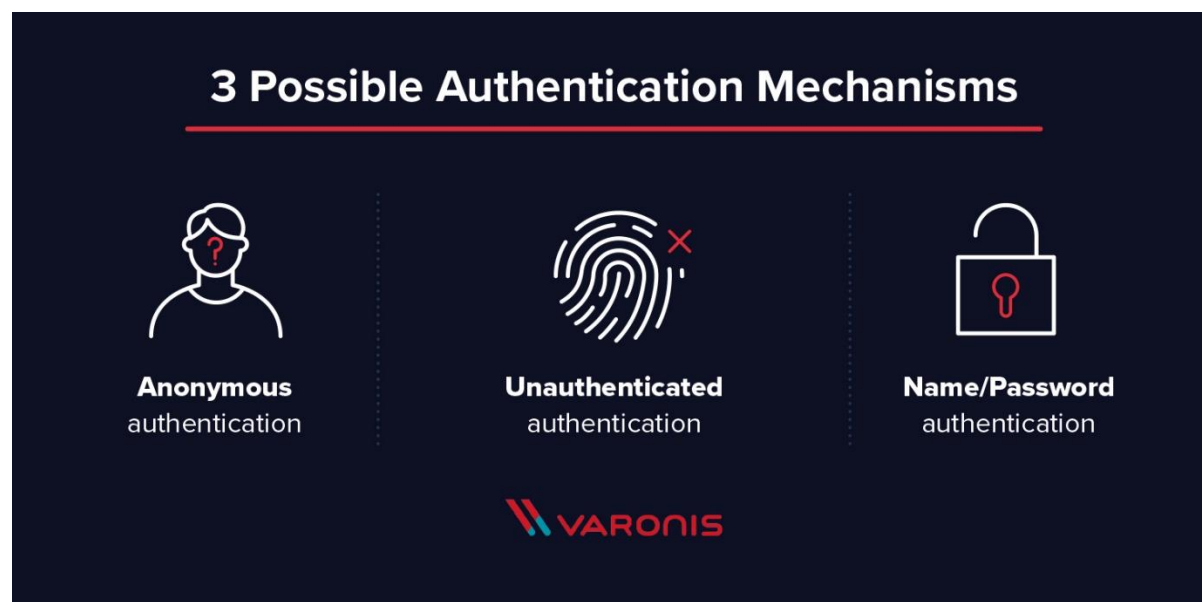


Figure 1. Simple Authentication mechanism

**Anonymous authentication:** Grants client anonymous status to LDAP (Sobers, 2018).

**Unauthenticated authentication:** For logging purposes only, should not grant access to a client (Sobers, 2018).

**Name/Password authentication:** Grants access to the server based on the credentials supplied – simple user/pass authentication is not secure and is not suitable for authentication without confidentiality protection (Sobers, 2018).

SASL authentication binds the LDAP server to another authentication mechanism, like Kerberos. The LDAP server uses the LDAP protocol to send an LDAP message to the other authorization service. That initiates a series of challenge response messages that result in either a successful authentication or a failure to authenticate.

## LDAP Query

An LDAP query is a command that asks a directory service for some information. For instance, if you'd like to see which groups a user is a part of, you'd submit a query that looks like this (Sobers, 2018):

**(&(objectClass=user)(sAMAccountName=yourUserName)**

**(memberof=CN=YourGroup,OU=Users,DC=YourDomain,DC=com))**

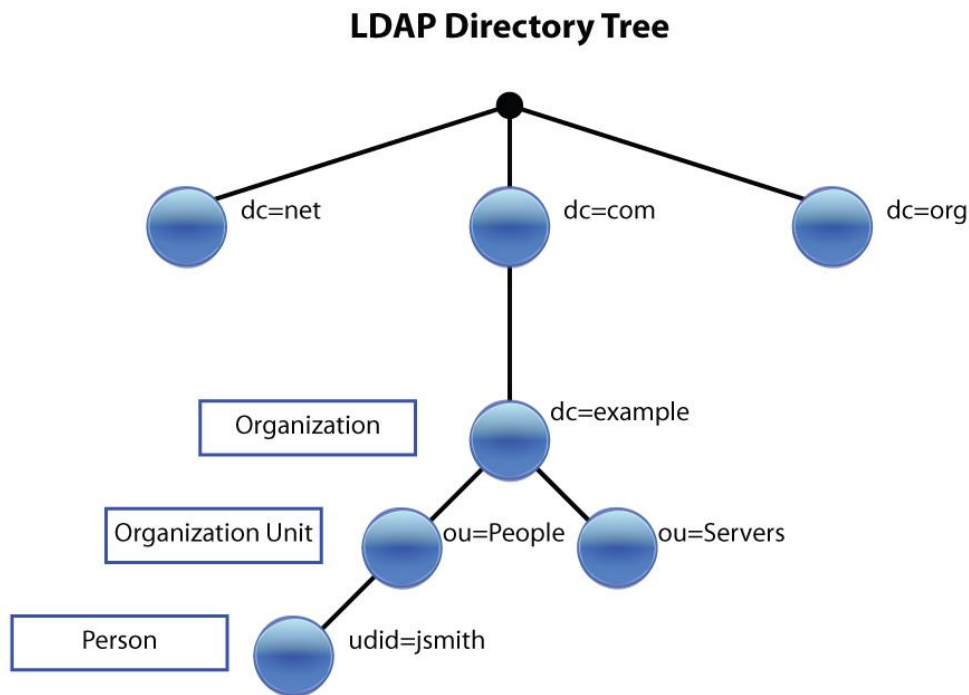


Figure 3. Workflow of LDAP

## DIRECTORIES IMPLEMENTATIONS

1. Microsoft Active Directory
2. NetIQ eDirectory
3. Sun Microsystems OpenDS
4. OpenLDAP
5. Apple open directory
6. Oracle Internet Directory
7. Apache Directory server

## Microsoft Active Directory

Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. Active Directory uses a structured data store as the basis for a logical, hierarchical organization of directory information (Flores, Billmath, Kumar, & Plett, 2017)

The data store (known as directory), contains all the information about Active directory objects. These objects include shared resources such as servers, volumes, printers and computer accounts (Flores, Billmath, Kumar, & Plett, 2017).

Security is integrated with Active Directory through logon authentication and access control to objects in the directory. With a single network logon, administrators can manage directory data and organization throughout their network, and authorized network users can access resources anywhere on the network (Flores, Billmath, Kumar, & Plett, 2017).

**Schema :** A set of rules, that defines the classes of objects and attributes contained in the directory, the constraints and limits on instances of these objects, and the format of their names (Flores, Billmath, Kumar, & Plett, 2017).

**Global Catalog:** It contains information about every object in directory. This allow users and administrators to find directory information regardless of which domain in the directory contains the data (Flores, Billmath, Kumar, & Plett, 2017).

**A query index information:** It is there because object and their properties can be published and found by network users or application (Flores, Billmath, Kumar, & Plett, 2017).

**Replication service:** It distributes directory data across the network. All domain controllers in a domain participate in replication and contain a complete copy of all directory information for their domain. Any change to directory data is replicated to all domain controllers in the domain (Flores, Billmath, Kumar, & Plett, 2017).

## Top Companies that uses Active Directory

- 1.JP Morgan Chase
2. Centrifify
3. Xantrion
4. Ricoh Co. Ltd.
5. First Republic Bank

Source:<https://idatalabs.com/tech/products/microsoft-active-directory-federation-services>

## Active Directory in Cloud

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service (Microsoft, 2018).

Azure AD helps your employees sign in and access resources in:

- External resources, such as Microsoft Office 365, the Azure portal, and thousands of other SaaS applications (Microsoft, 2018).
- Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization (Microsoft, 2018).

### Users of Azure Active Directory:

**IT admins.** As an IT admin, you can use Azure AD to control access to your apps and your app resources, based on your business requirements (Microsoft, 2018).

**App developers.** As an app developer, Azure AD gives you a standards-based approach for adding single sign-on (SSO) to your app, allowing it to work with a user's pre-existing credentials (Microsoft, 2018).

**Microsoft 365,** Office 365, Azure, or Dynamics CRM Online subscribers. As a subscriber, you're already using Azure AD. Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant (Microsoft, 2018).

### AWS Directory Service for Microsoft Active Directory

AWS Microsoft AD (Standard Edition) offers you a highly available and cost-effective primary directory in the AWS Cloud that you can use to manage users, groups, and computers (Pereira, 2017).

It enables you to join Amazon EC2 instances to your domain easily and supports many AWS and third-party applications and services. It also can support most of the common use cases of small and midsize businesses (Pereira, 2017).

When you use AWS Microsoft AD (Standard Edition) as your primary directory, you can manage access and provide single sign-on (SSO) to cloud applications such as Microsoft Office 365 (Pereira, 2017).

If you have an existing Microsoft AD directory, you can also use AWS Microsoft AD (Standard Edition) as a resource forest that contains primarily computers and groups, allowing you to migrate your AD-aware applications to the AWS Cloud while using existing on-premises AD credentials (Pereira, 2017).

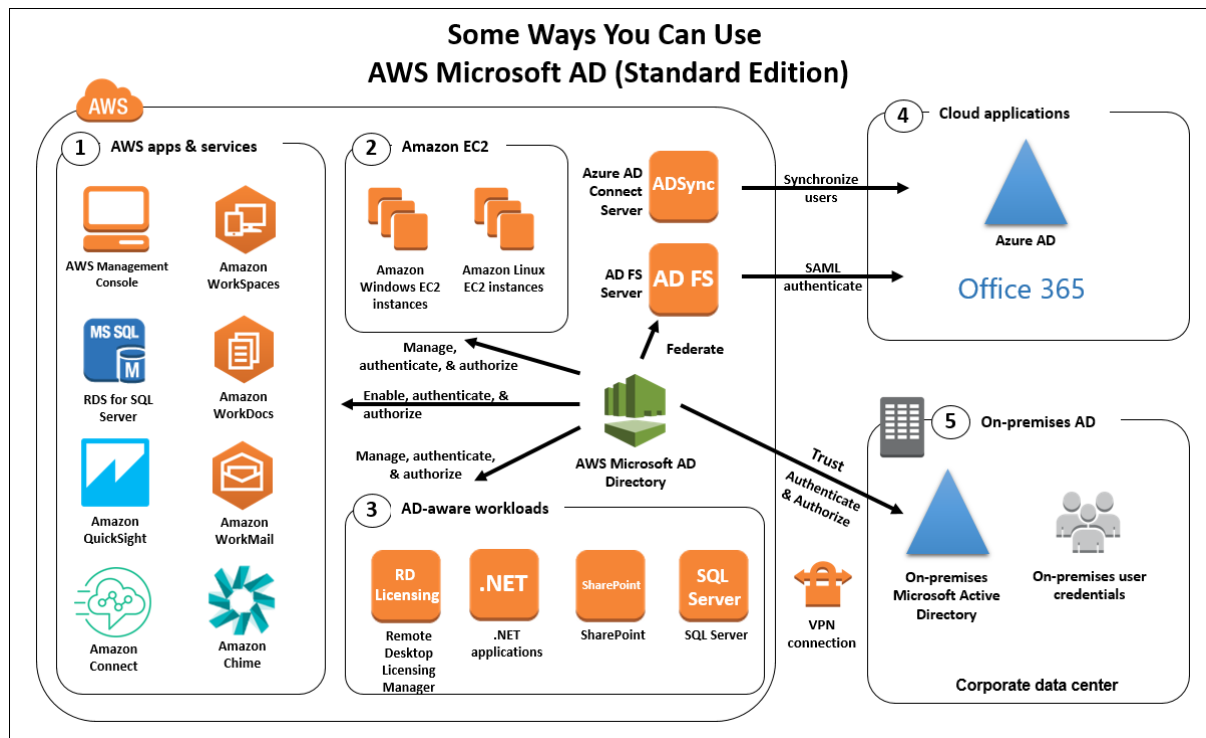


Figure 4. Way to use AWS Microsoft AD

## Strengths of Active Directory

- You can set up easily and use it.
- It will let you manage your network from one point.
- Identity management is simple as you can view all user information.
- The speed of providing domain name is faster.
- No need to provide usernames and passwords for outlook.
- Sharing resources such as files and printers is easier.
- Enables users to sign in using usernames and passwords.

## Weakness of Active Directory

- OS dependent as it needs windows server to work
- High Maintenance cost
- Prone to be hacked
- If active directory goes down, then whole network goes down.

# METHODOLOGY

## Penetration Testing on Active directory

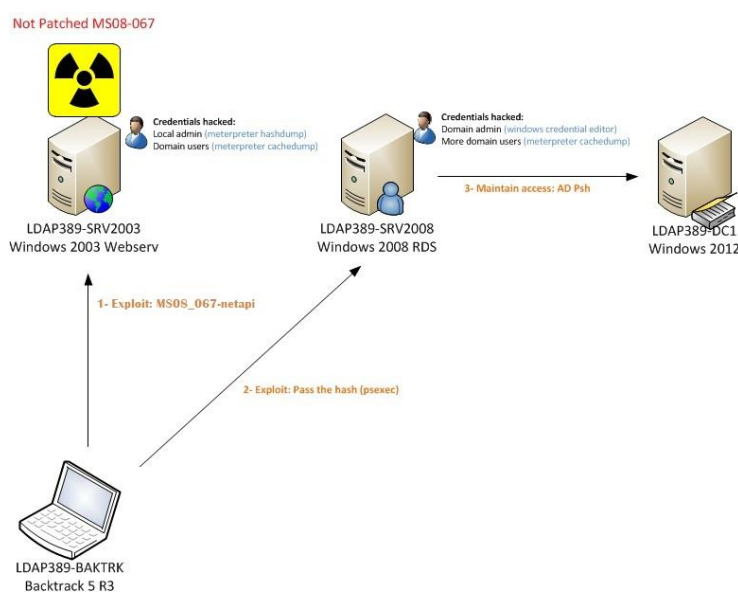
### 1. Scanning

The purpose of this step is to identify what computers are running in ADDS domain and which role and vulnerabilities are present on each computer. All the computers are in the same subnet. We launch the following Nmap command in order to launch the network scan (Savina, 2012).

Then we launch Nessus to scan all the vulnerabilities.

Note about the vulnerability scan (Nessus or Nmap): Always launch a safe scan otherwise you might crash the targeted OS (Savina, 2012).

We can now start the exploitation phase, because we have accurate information on the machines running on the domain, here is diagram of the intrusion scenario (Savina, 2012):



### 2. Exploitation

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. If the prior phase, vulnerability analysis was performed properly, this phase should be well planned and a precision strike. The focus is to

identify the main entry point into the organization and to identify high value target assets (GNU, 2019).

If the vulnerability analysis phase was properly completed, a high value target list should have been compiled. Ultimately the attack vector should take into consideration the success probability and highest impact on the organization (GNU, 2019).

## **Countermeasures**

Countermeasures are defined as preventative technology or controls that hinder the ability to successfully complete an exploit avenue. This technology could be a Host Based Intrusion Prevention System, Security Guard, Web Application Firewall, or other preventative methods. When performing an exploit, several factors should be taken into consideration. In the event of a preventative technology, a circumvention technique should be considered. In circumstances when this is not possible, alternative exploit methods should be considered (GNU, 2019).

Overall, the purpose is to remain stealth when attacking the organization, if alarms are tripped the level of the assessment could be diminished. If possible, the countermeasures should be enumerated prior to triggering the exploit. This could be done through doing dry runs of the attack or enumerating the technology (GNU, 2019).

## **Zero-Day Angle**

In most cases, the zero-day angle is often a last resort for most penetration testers. This type of attack often represents a highly advanced organization that can handle a focused attack against the organization through normal attack methods. In certain scenarios research may be conducted in order to reverse engineer, fuzz, or perform advanced discovery of vulnerabilities that have not been discovered. In the event this type of attack is applicable, ensure that the environment to the best of the attacker's knowledge is reproduced to include countermeasure technology (GNU, 2019).

In order for zero-day exploits to be successful (or any exploit for that matter), having the same operating system, patches, and countermeasures is highly important on success. Sometimes this information may not be available based on the level of access or enumeration that has occurred (GNU, 2019).

## **Fuzzing**

Fuzzing is the ability to recreate a protocol or application and attempt to send data at the application in hopes of identification of a vulnerability. Often the hopes of a fuzzer is to identify a crash in an application and craft a specific exploit out of it. In the case of fuzzing, the attacker is attempting to create a specific vulnerability out of something that hasn't been discovered before. As part of a penetration test, if no avenues are identified during the engagement, or the



engagement calls for zero-day research; fuzzing techniques should be leveraged in order to identify potentially vulnerable exposures (GNU, 2019).

## **Source Code Analysis**

Other avenues that a penetration tester has available is if the source code is available or open-source. If the tester has the ability to look at the source code and identify flaws within the application, zero-day exposures can also be identified through these methods (GNU, 2019).

## **Types of Exploits**

There are several types of exploits that can be identified during a penetration test that could be classified as a zero-day. Some are listed in this section (GNU, 2019).

### **Buffer Overflows**

Buffer overflows occur due to improper coding techniques. Specifically, this usually occurs when a program writes data to a buffer and then overruns the buffer's boundary and begins to overwrite portions of memory. In buffer overflow exploits the attacker's goal is to control a crash and gain code execution on the given system. In a buffer overflow exploit, one of the more common techniques is to overwrite a given register and "jump" to the shellcode (GNU, 2019).

### **SEH Overwrites**

SEH overwrites occur when the structured exception handler begins to gracefully close an application. The attacker can manipulate how SEH works, overwrite the base address of the SEH handler and gain control of execution flow through the SEH. This is a common attack leveraged with buffer overflow vulnerability and applications that have been complied with SEH (GNU, 2019).

### **Return Oriented Programming**

Return Oriented Programming (ROP) is a technique used during a portion where the user has control of execution flow however data execution prevention (DEP) or other precluding defense mechanisms may be in place. In the situation where DEP is enabled, the attacker does not have direct access to execute specific assembly instructions, therefor the attacker builds ROP gadget in order to prep certain Windows API calls or techniques to disable DEP or circumvent DEP. A common method is leveraging the WriteProcessMemory call to copy data from the stack into a writable memory space that can then be executed (GNU, 2019).

### **Traffic Analysis**

Traffic analysis is the technique of identifying what type of information is being sent and the ability to understand and manipulate that traffic. A penetration tester should be able to understand how a protocol works and how it can be manipulated in order to leverage an attack (GNU, 2019).

### **Physical Access**

Physical access during a penetration test can be a viable attack method for attempting to circumvent physical security controls and gain unauthorized access. During a penetration test, the assessor should be able to identify potentially flawed physical security controls and attempt to gain access to the facility if within scope (GNU, 2019).

### Human Angle

During a physical penetration test, some of the most obvious ways would be to social-engineer your way into the facility and gain access. This requires significant knowledge of how the organization performs business, and everything you learned from the intelligence gathering phase (GNU, 2019).

### PC Access

If physical access is granted to a PC, the penetration tester should be able to attack the PC and gain access through multiple methods that would allow access to the system (GNU, 2019).

### Proximity Access (WiFi)

Wireless communications are an avenue for attacks to gain access through RF type communications. The penetration tester should view the FCC radio frequency list to see if the target has registered spectrum frequencies in use (GNU, 2019).

### WiFi Attacks

Regardless of protocol, there are several attacks available for WEP, WPA, WPA2, EAP-FAST, EAP-LEAP, and other avenues. The attacker should be familiar with the various encryption protocols and standards and be able to effectively test the implementation around the controls put in place (GNU, 2019).

### Attacking the User

Leveraging rogue access points in order to attack the victim is often a beneficial and a viable attack method. Leveraging a rogue access point to entice victims in order to leverage exploits or steal sensitive information should be performed during a wireless assessment. There are several common techniques in use of this, but most commonly the attacker would setup a wireless access point with the same name or an enticing name for the victim to connect (GNU, 2019).

### 3. MAINTAIN ACCESS

In order to manipulate AD objects more easily it could be good to have the RSAT-AD-PowerShell feature installed on the ldap389-srv2008 machine. To install this feature, we will upload the Install-ADDS-PSH.ps1 script in our c:\tools directory and launch the script for the meterpreter shell (Savina, 2012).

```
c:\tools>powershell.exe -f install-ADDS-Psh.ps1
powershell.exe -f install-ADDS-Psh.ps1
Add-WindowsFeature : Because of security restrictions imposed by
User Account Control, you must run Add-WindowsFeature in a
Windows PowerShell session opened
with elevated rights. To do this, right-click the Windows PowerShell
or Command
Prompt Start menu object that you are using to start your Windows
PowerShell s
essions, and then click Run as administrator.
At C:\tools\install-ADDS-Psh.ps1:2 char:19
+ add-windowsfeature <<<< RSAT-AD-PowerShell + CategoryInfo
: PermissionDenied: (:) [Add-WindowsFeature], Exce ption +
FullyQualifiedErrorId :
NotAdministrator,Microsoft.Windows.ServerManager
.Commands.AddWindowsFeatureCommand
```

Here is the PowerShell script:

```
import-module servermanager
add-windowsfeature RSAT-AD-PowerShell
```

Once the RSAT-AD-PowerShell feature is installed we can migrate with the meterpreter to a process running under the ldap389\domainadm account and launch Powershell scripts with the ADDS cmdlets (Savina, 2012).

One obvious solution to maintain the access would be to create a new account member of the domain administrators' group and set up password never expires on that account. But this solution is not discreet because the members of this group are generally monitored (Savina, 2012).

Instead we will modify the ACL of the AdminSDHolder object, and grant modify rights for the user0001/user0001 account we cracked during the 2) exploitation phase. This account is modified so that its password never expires, generally a user will never complain or report this to the IT department (Savina, 2012).

So why modify this object in AD? The AdminSDHolder object has a unique ACL, which is used to control the permissions of built-in privileged Active Directory groups and their members, for those objects the adminCount attribute equals 1. If this protection process finds that security is different on the protected object than on the AdminSDHolder object, it will force AdminSDHolder's ACL on it (Savina, 2012).

The domain administrators group and the ldap389\domainadm account are protected objects, so if we modify the AdminSDHolder ACL, the ACL will be also modified on those two objects (Savina, 2012).

In order to set “password never expires” for the test0001 account and add the permissions for this account on the AdminSDHolder object we use the hack-ADDS-ps1.ps1 script, this post helped me to play with ACLs (Savina, 2012).

## **How to perform Audit?**

### **Step 1: Survey and Analyse**

Step one is to scan and map your AD environment to answer questions like (Fai, 2016):

- How many accounts and groups do you have?
- What kinds of toxic conditions exist?
- Who has permissions to your domain controllers (DCs) and organizational units (OUs)?

Once you know what's in your AD environment, you can start to triage (Fai, 2016).

### **Step 2: Focus on What Matters Most**

Step two is prioritizing efforts based on your findings. Three places organizations often begin are:

- Privileged AD Access—Examine critical objects like group policy and domain/enterprise admins (Fai, 2016).
- Large Group Remediation—Evaluate groups that in effect have the same membership as well-known security principles like all Domain Users or the Everyone groups (Fai, 2016).
- Privileged User Access—Determine which users have elevated or direct access (Fai, 2016).

### **Step 3: Get the Right Stakeholders Involved**

Step 3 is gaining support to address priority issues. You can use permissions scans data, for instance, to identify stakeholders based on who has access within Active Directory—as well as who has access to Active Directory objects. For example, you can identify the manager of groups or users who will know why permissions have been set-up a certain way, e.g., delegated admin permissions to perform certain tasks like resetting passwords (Fai, 2016).

### **Step 4: Review and Remediate**

With stakeholders onboard, you can review group memberships and remediate problematic AD conditions. First, remediate privileged access to AD by verifying that the right users are in domain and enterprise admins. This least privilege approach reduces the chance that a rogue admin will abuse privileges by accessing sensitive data or adding an unauthorized user to the group's membership. Second, involve business owners in group governance to help validate that the right members are in their groups—and that the group overall has access to the resources it needs (Fai, 2016).

### **Step 5: Make the Process Repeatable**

Step five is making the process a continuous cycle. Once you complete your top priorities, you return to step one and repeat the process for your next priority. For example, another focus area might be ensuring AD passwords follow change policies and aren't stored in memory (Fai, 2016).

## IMPLEMENTATION AND RESULTS

If you perform regular vulnerability scans and discover that your LDAP server suffers from these issues, what do they mean?

### **NULL Base Search**

An LDAP server that allows a NULL base search means that the attacker does not need to know a base object before querying. A very good explanation can be found here (Blogger, 2013):

“LDAP implementations are required to return some information as a result of a search. This information is required for LDAP clients to bind and interact with the directory. When this event occurs, users can dump the base of the tree or issue a request without knowing the base object. LDAP implementations vary on how or whether it is possible or necessary to constrain or prevent NULL base requests. Some implementations use an access control list (ACL), others provide the ability using a utility program or user interface, and others may not be able to prevent these requests.” (Blogger, 2013)

Source: [http://www.iss.net/security\\_center/reference/vuln/ldap-nullbase.htm](http://www.iss.net/security_center/reference/vuln/ldap-nullbase.htm)

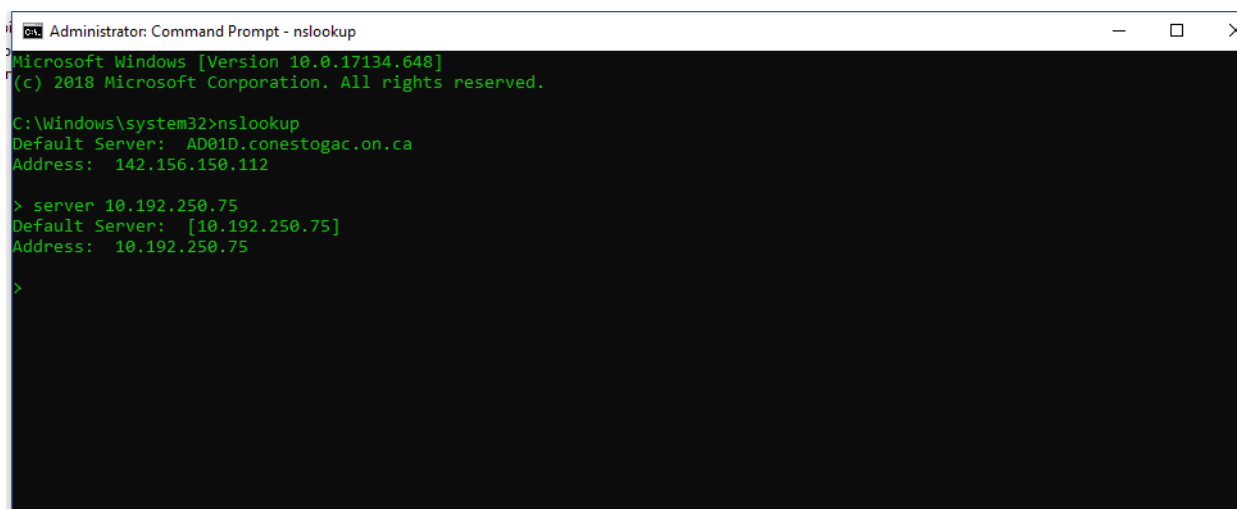
### **NULL/Anonymous Bind**

An LDAP server that allows anonymous binds does not require any type of credentialed authentication (Blogger, 2013).

“The NULL bind entry allows a user to access the Lightweight Directory Access Protocol (LDAP) directory anonymously. An attacker could take advantage of the NULL bind entry to anonymously view files on the LDAP director. (Blogger, 2013)”

Source: [http://www.iss.net/security\\_center/reference/vuln/ldap-nullbind.htm](http://www.iss.net/security_center/reference/vuln/ldap-nullbind.htm)

## 1. Reconnaissance



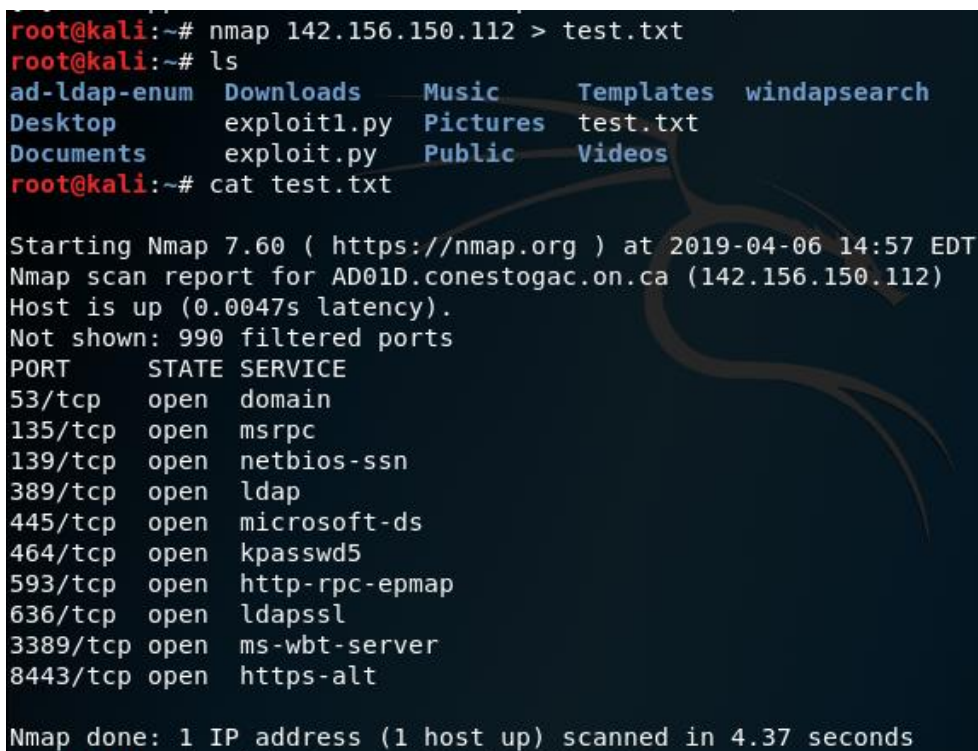
```
Administrator: Command Prompt - nslookup
Microsoft Windows [Version 10.0.17134.648]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nslookup
Default Server:  AD01D.conestogac.on.ca
Address:  142.156.150.112

> server 10.192.250.75
Default Server:  [10.192.250.75]
Address:  10.192.250.75

>
```

Figure 1. Finding IP Address of Conestoga's Active Directory



```
root@kali:~# nmap 142.156.150.112 > test.txt
root@kali:~# ls
ad-ldap-enum  Downloads  Music      Templates  windapsearch
Desktop       exploit1.py Pictures    test.txt
Documents     exploit.py  Public     Videos
root@kali:~# cat test.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2019-04-06 14:57 EDT
Nmap scan report for AD01D.conestogac.on.ca (142.156.150.112)
Host is up (0.0047s latency).
Not shown: 990 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
389/tcp    open  ldap
445/tcp    open  microsoft-ds
464/tcp    open  kpasswd5
593/tcp    open  http-rpc-epmap
636/tcp    open  ldapssl
3389/tcp   open  ms-wbt-server
8443/tcp   open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 4.37 seconds
```

Figure 2. Scanning for Open ports

After that we performed Nessus scan on the IP address of Active directory.

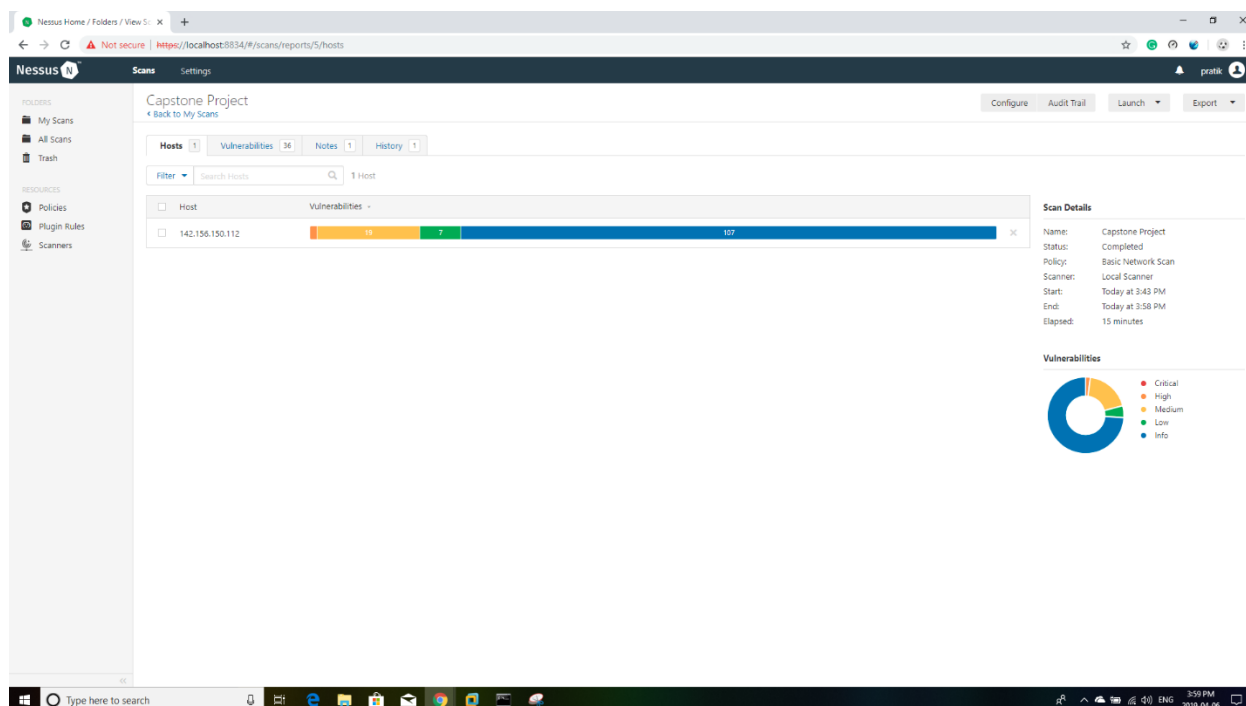


Figure 3. Full Nessus scan

If we click on vulnerabilities, we can see all the vulnerabilities of the server.

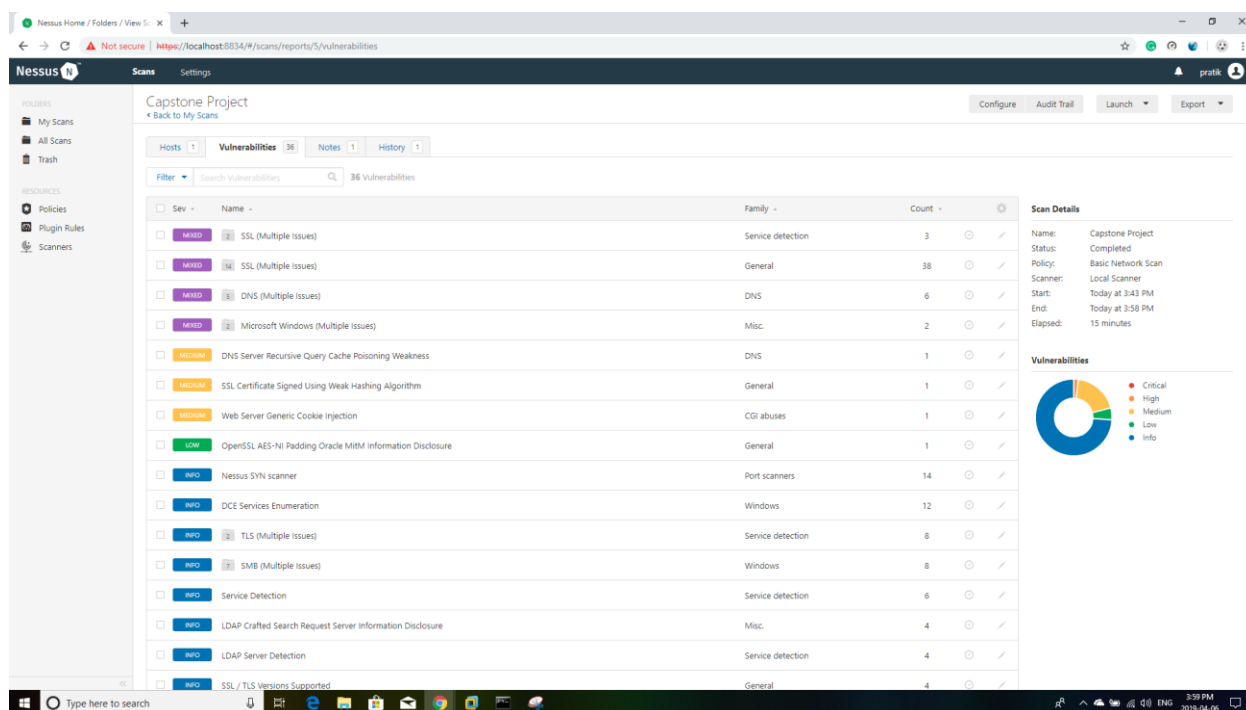




Figure 4. Lists of vulnerabilities

Then we tried LDAP injection and obviously it did not work as we know most of things are safe from injection attack in 2019.

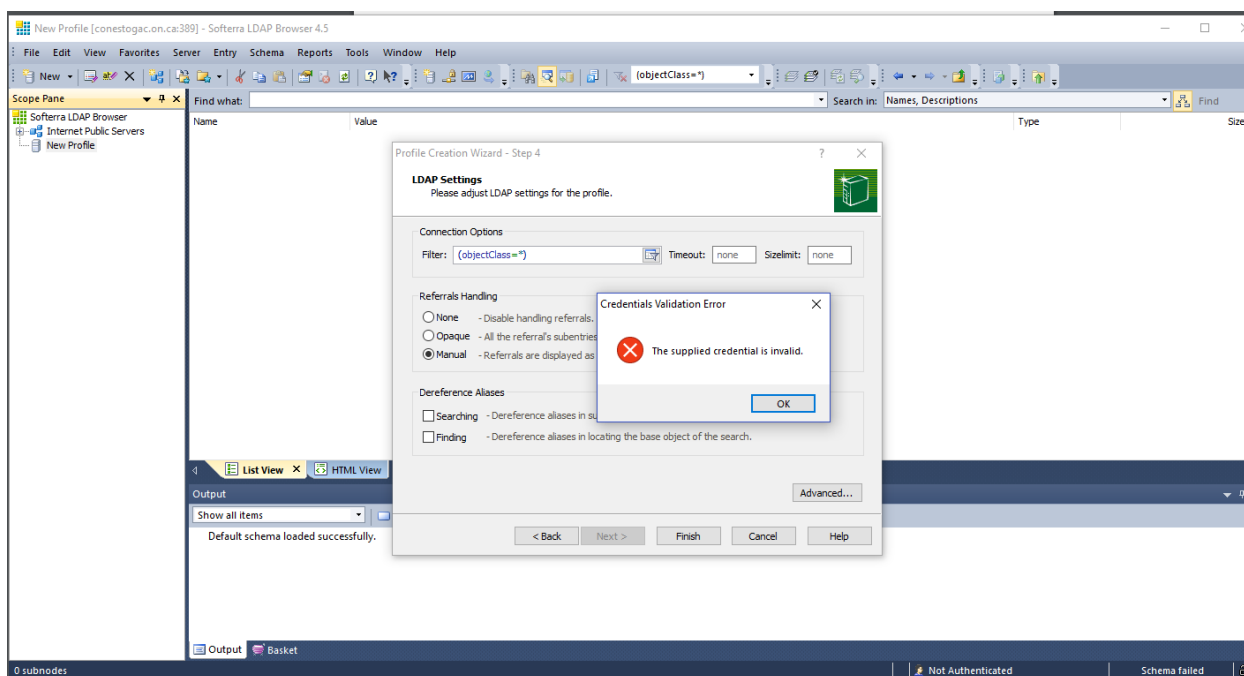
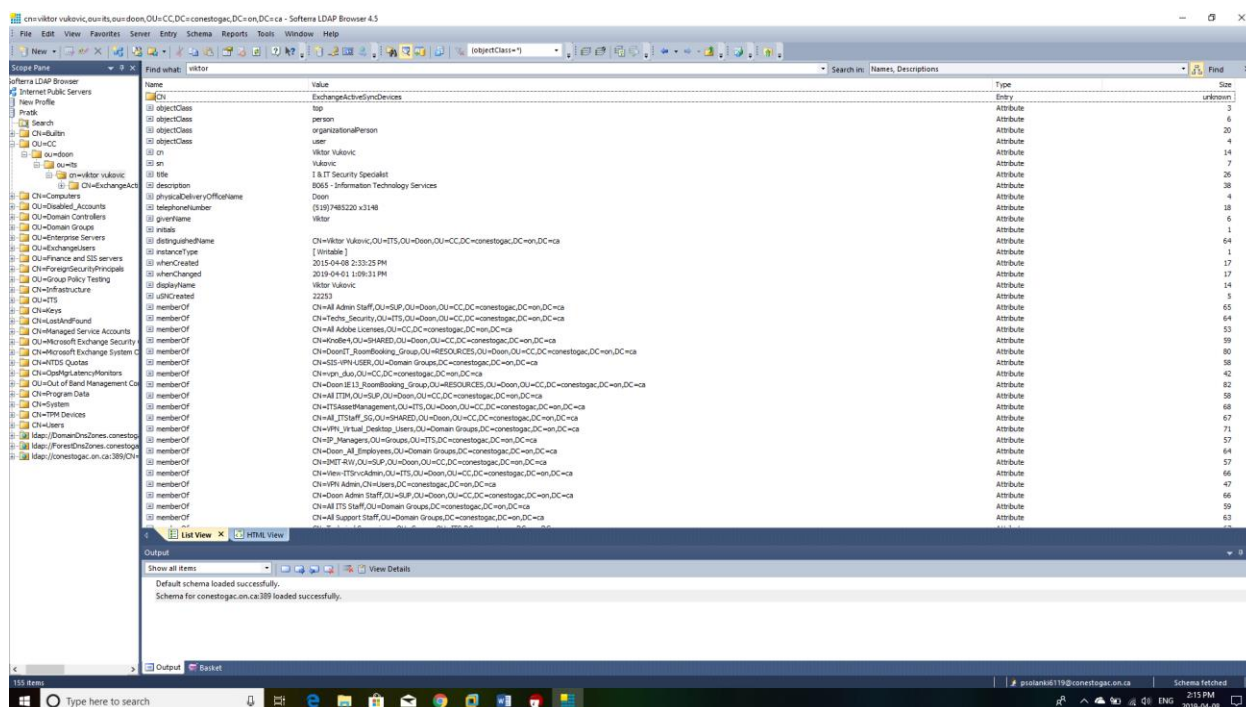


Figure 5. LDAP Injection

ObjectiClass Vulnerability.



There are other 4 attacks that work on active directory, but they are very dangerous, so we did not try them, but they are listed below.

## 1. Exploiting Weak Permissions

```
PS C:\PowerSploit-master> Invoke-ACLScanner

ObjectDN      : CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=JEFFLAB,DC=local
ObjectSID     : 
IdentitySID   : S-1-5-21-2490182989-4136226752-3308112936-1112
ActiveDirectoryRights : GenericAll
InheritanceType : All
ObjectType    : 00000000-0000-0000-0000-000000000000
InheritedObjectType : 00000000-0000-0000-0000-000000000000
ObjectFlags   : None
AccessControlType : Allow
IdentityReference : JEFFLAB\Tobias
IsInherited   : False
InheritanceFlags : ContainerInherit, ObjectInherit
PropagationFlags : None

ObjectDN      : CN=User,CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=JEFFLAB,DC=local
ObjectSID     : 
IdentitySID   : S-1-5-21-2490182989-4136226752-3308112936-1112
ActiveDirectoryRights : GenericAll
InheritanceType : All
ObjectType    : 00000000-0000-0000-0000-000000000000
InheritedObjectType : 00000000-0000-0000-0000-000000000000
ObjectFlags   : None
AccessControlType : Allow
IdentityReference : JEFFLAB\Tobias
IsInherited   : True
InheritanceFlags : ContainerInherit, ObjectInherit
PropagationFlags : None

ObjectDN      : CN=Machine,CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=JEFFLAB,DC=local
ObjectSID     : 
IdentitySID   : S-1-5-21-2490182989-4136226752-3308112936-1112
ActiveDirectoryRights : GenericAll
InheritanceType : All
ObjectType    : 00000000-0000-0000-0000-000000000000
InheritedObjectType : 00000000-0000-0000-0000-000000000000
ObjectFlags   : None
AccessControlType : Allow
IdentityReference : JEFFLAB\Tobias
IsInherited   : True
InheritanceFlags : ContainerInherit, ObjectInherit
PropagationFlags : None
```

## 2. Attacking AD permissions with Blood hound

```
PS C:\Bloodhound\BloodHound-master\BloodHound-master\PowerShell> Invoke-Bloodhound -CollectionMethod ACLs
Writing output to CSVs in: C:\Bloodhound\BloodHound-master\BloodHound-master\PowerShell\
Done writing output to CSVs in: C:\Bloodhound\BloodHound-master\BloodHound-master\PowerShell\
```

## 3. AdminSDHoleder and SDProp

```
1  $ldapFilter = "(adminCount=1)"
2  $domain = New-Object System.DirectoryServices.DirectoryEntry
3  $search = New-Object System.DirectoryServices.DirectorySearcher
4  $search.SearchRoot = $domain
5  $search.PageSize = 1000
6  $search.Filter = $ldapFilter
7  $search.SearchScope = "Subtree"
8
9  $results = $search.FindAll()
10
11 foreach ($result in $results)
12 {
13     $userEntry = $result.GetDirectoryEntry()
14     Write-host "Object Name = " $userEntry.name
15     Write-host "Object Class = " $userEntry.objectClass
16     foreach($adminCount in $userEntry.adminCount)
17     {
18         Write-host "AdminCount =" $adminCount
19         Write-host ""
20     }
21 }
22 }
```

## 4. Unconstrained Delegation Permissions

```

Authentication Id : 0 ; 3088503 (00000000:002f2077)
Session          : Network from 0
User Name        : Administrator
Domain           : JEFFLAB
Logon Server      : (null)
Logon Time       : 6/26/2017 7:16:32 AM
SID              : S-1-5-21-2490182989-4136226752-3308112936-500

* Username : Administrator
* Domain   : JEFFLAB.LOCAL
* Password : (null)

Group 0 - Ticket Granting Service
Group 1 - Client Ticket ?
Group 2 - Ticket Granting Ticket
[00000000]
Start/End/MaxRenew: 6/26/2017 7:15:48 AM : 6/26/2017 5:15:46 PM : 7/3/2017 7:15:46 AM
Service Name (02) : krbtgt ; JEFFLAB.LOCAL ; @ JEFFLAB.LOCAL
Target Name (--) : @ JEFFLAB.LOCAL
Client Name (01) : Administrator ; @ JEFFLAB.LOCAL
Flags 60a10000 : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
Session Key     : 0x00000012 - aes256_hmac
9438970035fac5a859e518b67de70b5bce827a44753a1af8a68ecc1f35c333b8
Ticket          : 0x00000012 - aes256_hmac ; kvno = 4 [...]
* Saved to file [0;2f2077]-2-0-60a10000-Administrator@krbtgt-JEFFLAB.LOCAL.kirbi !

```

## Conclusion

We have shown that why security of Active directory is very important. As we know that most of the organizations stores their data on active directory servers it becomes most favorite target of attackers.

We found that there is “ObjectClass” vulnerability in LDAP port 389. The vulnerability does not look very risky at first place, but it may lead to different types of attacks.

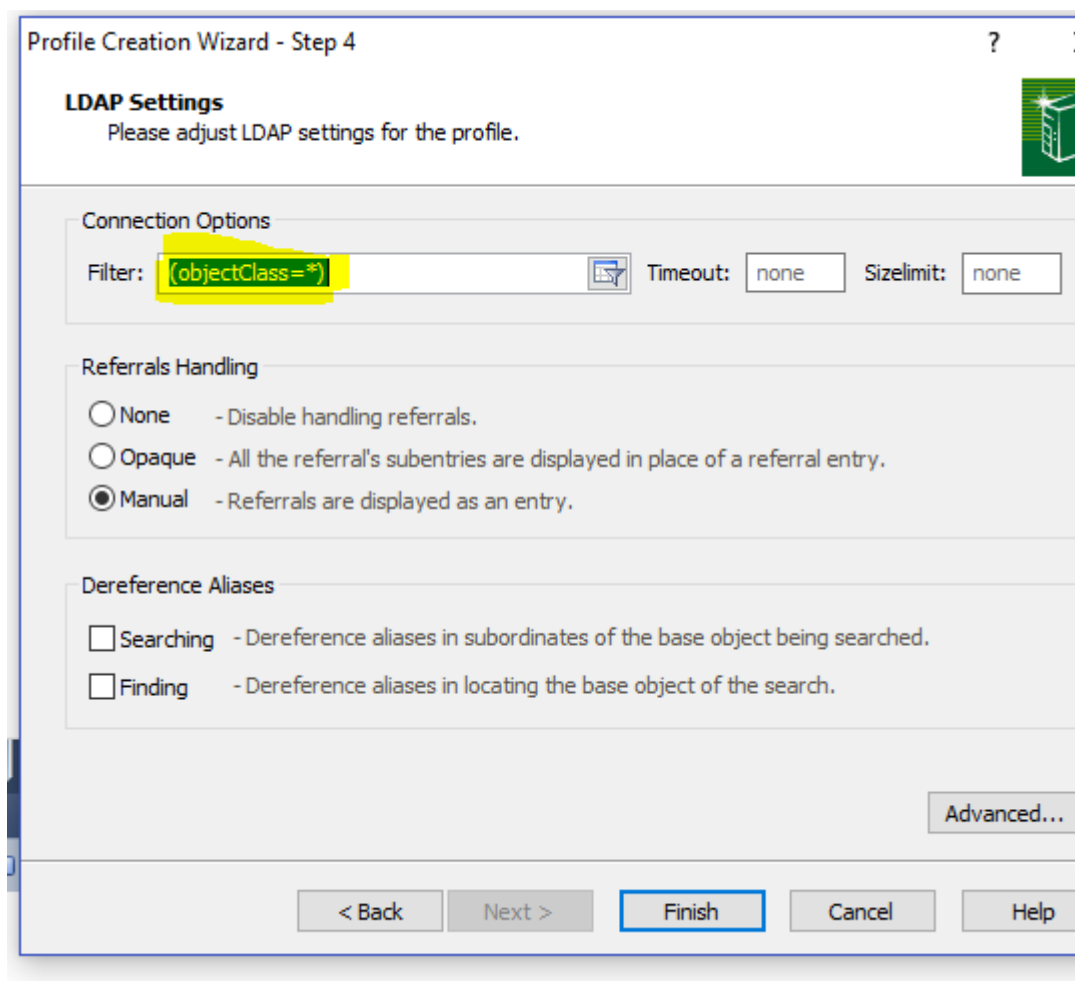


Figure 1. Object Class vulnerability

So, if an attacker wants to gain access then he installs malware in user's computer that will take all the inputs from user and send it to attacker via network activity. From that keystrokes the attacker can easily find user's log in information to look for other user's information and after that he does social engineering attack to all the other users.

The main solution to stick away from attacker is doing audit of active directory frequently. If audit is performed, then we can keep track of every unusual activities and then possibly find the attacker.

Another solution is to store all active directory data to the cloud. Cloud will add one more layer of security and it will be difficult for intruder to breach the data from cloud.

## 6. References

- Howard Solomon (2016, January 21). IT not doing enough to secure Active Directory. Retrieved from <https://www.itworldcanada.com/article/it-not-doing-enough-to-secure-active-directory-says-expert/380201>
- CrowdStrike. Active Directory Assessment. [https://www.crowdstrike.com/wp-content/brochures/datasheets/Datasheet\\_Active\\_Directory\\_Security\\_Assessment\\_v.03.09.18.pdf](https://www.crowdstrike.com/wp-content/brochures/datasheets/Datasheet_Active_Directory_Security_Assessment_v.03.09.18.pdf)
- Beyond Trust. <https://www.beyondtrust.com/resources/glossary/active-directory-security>
- <https://merabheja.com/22-best-alternatives-to-microsoft-active-directory/>
- Fai, T. (2016, 12 20). *BEST PRACTICES FOR AUDITING ACTIVE DIRECTORY*. Retrieved from INSIDER THREAT SECURITY BLOG: <https://blog.stealthbits.com/best-practices-for-auditing-active-directory>
- Flores, J., Billmath, Kumar, S., & Plett, C. (2017, 05 30). *Active Directory Domain Services Overview*. Retrieved from <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>
- LDAP.com. (2019). *LDAP.com Lightweight Directory Access Protocol*. Retrieved from <https://ldap.com/>
- Microsoft. (2018, 12 11). *What is Azure Active Directory?* Retrieved from Microsoft Azure: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-what-is>
- Netwrix. (2019). *Complete visibility into what's going on in your*. Retrieved from NetWrix: [https://www.netwrix.com/active\\_directory\\_auditing.html](https://www.netwrix.com/active_directory_auditing.html)
- GNU. (2019). *Exploitation*. Retrieved from <http://www.pentest-standard.org/index.php/Exploitation>
- Savina, L. (2012, Dec 12). *Pentesting an Active Directory infrastructure*. Retrieved from <https://www.ldap389.info/en/2012/12/10/pentesting-active-directory-hacking/>
- Blogger. (2013, September 30). *SecuritySynapse*. Retrieved from <http://securitysynapse.blogspot.com/2013/09/>
- STEALTHbits. (2019). *INSIDER THREAT SECURITY BLOG*. Retrieved from <https://blog.stealthbits.com/unconstrained-delegation-permissions/>