WHITE PAPER

Hacking Active Directory – From a Pen Tester

Presented by

Active Directory provides authentication and protects credentials, information systems and intellectual property from unauthorized access, which in turn protects your organization's bottom line and reputation.

Globally, more than 95 percent of Fortune 1000 companies rely on Active Directory (AD) for authentication and single-sign-on support for their user populations. As it is nearly everywhere – in every company, organization and government agency – this makes AD a primary target for attackers looking to steal your intellectual property, your customer data or to hold your data for ransom.

Active Directory has changed significantly since its initial rollout in 2000, including both in technology and in how it is used. Years ago, it was focused on connecting to internal resources, file shares, mapped drives and printers. Today's office may still use many of these functions but have added services that take AD outside of the office walls. Cloud services, such as Office 365 and cloud-provided applications, change the way work is done and how AD connects all this information.

Black Hats and White Hats have many methods to achieve their goals. This ranges from highly technical long-term exploits to simple and obvious oversights. Here are some of the most typical AD-specific exploits seen today.

Password spraying

Password spraying is a common attack since most organizations either use an external resource or make internal resources available externally. This can be any publicly facing web page or other systems that use AD for authentication. Outlook Web Access is typical in most organizations and can be vulnerable to these attacks.

With password spraying, an attacker will have tables and lists of previously compromised passwords and cracked hashes. They will continuously and methodically inject these to an authentication web page or other system. Since most systems are designed to lock out accounts after a few failed logon attempts, the attacker will usually rotate usernames. Instead of finding

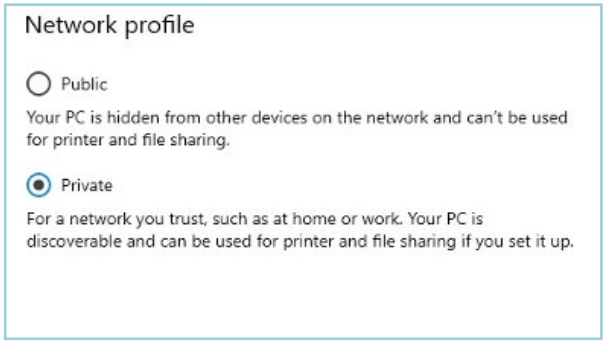
a password that fits a username, think of this as finding a username that fits a password. A single failed logon against one user account doesn't usually raise any red flags. Once the attacker has the username and password, they now have access to any resource that the user does. This means the attacker now has access to any intellectual property, customer lists or database for which the user is authorized. Moreover, if the user has privileged access, so does the attacker.

Password spraying remediations

- Use good password hygiene. Again, password complexity slows down the cracking process significantly. Users can be trained to use good passwords but technical controls to enforce them are much more effective. One Identity's Password Manager not only offers the users the ability to reset AD passwords and unlock accounts but it can enforce password complexity based on policies. This allows you to have different password policies for different types of accounts. One Identity's Password Manager validates user-password resets with a credential-verification service. This service compares the requested password with known compromised passwords that are from the same list the attackers use. If it matches, the user must choose a different or stronger password.
- Multifactor Authentication (MFA) is another great way to protect accounts. Beyond just the username/password combo, which can be shared and easily compromised, MFA adds another step to the authentication process to prevent malicious use and compromise of the resources being protected. Defender from One Identity leverages AD to accelerate and simplify MFA. Users can request and manage physical or soft tokens through a web interface, which takes the administrative workload of MFA from the admins.

LLMNR – Local Loop Multicast Name Resolution

It sounds complicated but it's simple. Windows systems broadcast to see if a computer system they are looking for is on their local network. This is like when you're looking for someone in a crowded room, so you stand on a chair and yell their name (but on the network).



One exploit for LLMNR is done when Internet Explorer is set to use 'Automatic Proxy'. When this is checked, IE starts and will look for a host named 'WPAD'. An attacker can create a web server named 'WPAD' and set it for Windows Authentication.

An attacker will set up a 'listener' with a tool such as Metasploit. When a system broadcasts for the address of the WPAD system, the attacker's system will respond with "Hey, that's me! Who are you and what are your credentials?" Of course, the system will respond with an NT authentication challenge. Now the attacker has the hash.

Another way to use this exploit is when users attempting to access resources on the network but have a name wrong. In other words, if a user is looking for '\\server1\data' but types '\\sevrer1\data' their workstation will broadcast to look for the misspelled name. The attacker can quickly grab that info and use it to emulate the misspelled name, then challenge for authentication. Now they have the hash.

The next step is to turn the hash into a password. The attacker will probably take this offline to a powerful system and use a tool such as 'John the Ripper' or 'Hashcat'. Some systems with powerful graphics cards allow the cracking to be offloaded to this card for faster processing. It's not a question of 'if it will be cracked?' it's a matter of 'when?' Any password hash is potentially breakable – given enough time and CPU cycles. The goal is to make it not worth the effort

LLMNR exploit remediations

- Disable multicast name resolution on your domain. This can be done through a GPO setting (Computer Configuration -> Administrative Templates -> Network -> DNS Client) then select 'Turn off multicast name resolution). This setting will vary per operating system, but it basically prevents the computers from asking each other for resources without resolving names through DNS.
- Complex passwords can slow the success rate of an LLMNR exploit. The well-known password speech has been going on for years telling us how we must use unique and complex passwords for every system we access but we shouldn't write any of them down. ☻ Easy enough? In this case, the attacker is cracking a hash of a password. Each additional character in the password makes the task exponentially more difficult, so it takes more time. It's also important to remember that when passwords are changed, residual hashes become useless.
- Use multifactor authentication for your user population. MFA is a powerful tool used to prevent many types of authentication attacks by prompting the user for something more than just a password. Most of the time this is done with a one-time password from a physical or software token. In this case, even if an attacker retrieves a hash, then cracks it, it is not usable without the second factor. One Identity offers Defender, which enhances security by

requiring two-factor authentication to gain access to your network resources. Defender uses your current identity store within Microsoft Active Directory (AD) to enable two-factor authentication.

Default Credentials

Default credentials have been and will continue to be an access point for many attacks because it's easy. Software, systems, printer and appliances that provide a valuable resource to network users will quickly become a point of entry for attackers if they are even connected to a live network before changing the default credentials.

This is an open invitation. If an attacker can take control of a network device with a default admin credential, then listening for users to authenticate becomes easy. Consider a device such as a network printer. In an AD environment, this printer will usually authenticate users against AD to allow printing. An attacker that takes control of this printer will point the authentication to a listener, just like in LLMNR. Then credentials can be captured and cracked.

Default credential remediations

- Immediately change all default credentials before deployment of any system, appliance, printer or whatever device.
- Manage credentials with One Identity Safeguard for Privileged Passwords. This solution will randomize passwords on systems and vault the passwords. If you should need to use the password, it can be checked out, used, checked back in and changed. One Identity Safeguard for Privileged Passwords cycles passwords on systems on your interval to ensure compliance requirements are met.

Hardcoded credentials

Hardcoded credentials are a similar problem to default credentials. When an attacker gains access to a system, they will look through scripts and scheduled tasks. Most of these need to authenticate to run so the scripter will include the username/password in the script. The script or task may even need elevated permissions in a system to perform its task. Just like default credentials, these are easily grabbed by an attacker and used to exploit or move through resources looking for valuable data.

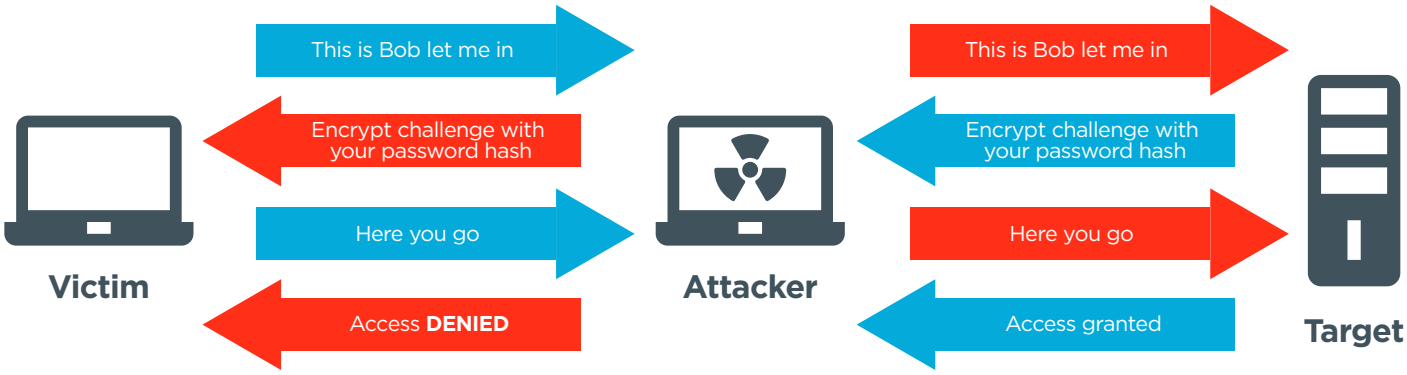
Hardcoded credential prevention

- All credentials that are either privileged or shared must be vaulted in a Privileged Account Management solution. One Identity Safeguard for Privileged Passwords provides for application-to-application check out of credentials for this type of scenario.
- The next task is to train scripters and coders to NOT use hard-coded credentials but utilize Safeguard for Privileged Passwords to manage credentials. DO NOT use hard-coded passwords in scripts or scheduled tasks.

SMB relaying

SMB relaying is a classic man-in-the-middle attack and after hundreds of penetration tests, it seems to never go away. The attack works by placing an attacker in the middle of an NTLM challenge/response protocol. The attacker listens for information across the network, points your authentication request to an asset of their choosing, acts as a middleman until access is granted and then they take it for themselves. The user attempting to authenticate will be denied and simply think they have entered in the wrong credentials and can attempt to connect again without issue. This can quickly land a malicious actor on sensitive machines with little to no effort.

You can think of it as a network version of pass-the-hash in that there is no password cracking, simply relaying of credential-based information. As with all attacks that reap great rewards, toolsets are created to make ease of exploitation rampant and SMB relaying is no exception. Attackers can execute this style of attack within moments of connecting to a target network.



SMB replay prevention/remediations

- Enable SMB Signing. This signs the packet to determine its authenticity. However, it does create overhead on the network and may break some legacy items. Certain environments may have to perform network segmentation if legacy assets are affected.
- Disable multicast name resolution on your domain. This can be done through a GPO setting (Computer Configuration -> Administrative Templates -> Network -> DNS Client) then select 'Turn off multicast name resolution). This setting will vary per operating system, but it basically prevents the computers from asking each other for resources without resolving names through DNS.
- Prevent WPAD poisoning with DNS entries that direct clients to the Internet.

Kerberoasting

Kerberoasting is an attack against service accounts in AD that use the 'ServicePrincipalName' or SPN attribute on a user object. Services that are set to authenticate against AD, such as Microsoft SQL, 'publish' their SPNs to their AD object. These service accounts are usually members of some privileged groups as well, making them more likely to be targeted.

The attackers use a valid domain user's Ticket Granting Ticket (TGT) to request service tickets from the domain controller. The domain controller returns service tickets for service principal names (SPNs) with the NTLM password hash for the service account tied to the ticket. These NTLM password hashes are vulnerable to offline cracking.

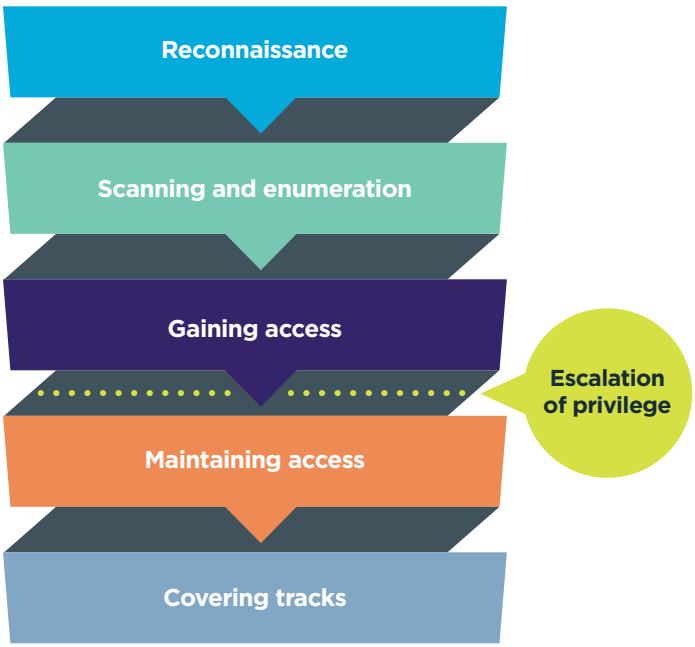
Kerberoasting prevention

- The first step is knowing which user objects are subject to this attack. Quest Enterprise Reporter will query AD and organize the data in any way you can imagine. Use Enterprise Reporter to gather all user information, then run a report where the 'ServicePrincipalName' has data. This will show you the user objects that can be attacked with Kerberoasting.
- You can prevent user objects from becoming vulnerable by alerting when the 'ServicePrincipalName' attribute is populated. Quest Change Auditor for AD audits not only audits all changes to AD but can be set to alert when certain changes happen. Turning on an alert for this will bring visibility to accounts that need extra protection. Additionally, Change Auditor for AD can protect objects and attributes from modification. The 'ServicePrincipalName' attribute can be protected from modification to prevent any more accounts from becoming vulnerable.
- Since service accounts cannot use MFA, password discipline is essential. Accounts vulnerable to Kerberoasting should have passwords with higher complexity, usually at least 25 characters. Tools such as One Identity Active Roles can dynamically build a group for these objects and add any new vulnerable objects to the group; then Safeguard for Privileged Passwords can control and vault complex passwords for these objects to make then as secure as possible.

Privilege Elevation in AD

Privilege Elevation in AD may not be the start of an attack but is usually a symptom that should sound alarms. If a standard user account has been compromised, the goal then is to compromise an account with elevated privileges, such as a Domain Admin. This, of course, gives the attacker access to all the resources with the ability to take or break anything, or even hold the AD for ransom.

Privilege elevation is part of nearly every attack (except for default credentials when the attacker walks in the front door with elevated privileges). The attacker works to elevate privileges immediately after gaining access.



Many organizations have widespread use of elevated privileges and no real visibility into who has them or what they are doing day-to-day. The privileged or VIP groups must be controlled and closely monitored for membership and access. Often other groups are nested within these VIP groups, which adds to the complexity of the vulnerability.

Privilege elevation prevention and remediation

- You need to know where the elevated privileges are before you can form a plan to prevent problems. Use Quest Enterprise Reporter to analyze the permissions and group memberships of your Active Directory to gain an understanding of the current state, and what you can do to reduce your attack surface.
- Closely monitor changes to permissions, privileged groups and user objects, which are members of privileged groups. An attacker will attempt to compromise an account that is a member or add a compromised account to a privileged group. Monitoring and alerting on changes to these objects using Quest Change Auditor immediately send notification if an unauthorized change occurs.
- Prioritize protecting of privileged objects in AD. Quest Change Auditor for AD provides the ability to protect objects and attributes. Use this solution to protect the 'members' attribute of privileged groups. This will prevent an attacker from adding members to the privileged groups and alert if an attempt is made. As a side note, you should also protect GPOs that have far-reaching scopes. An attacker can use Group Policy to spread ransomware. Consider protecting at least the Default Domain GPO and the Default Domain Controllers GPO from modification.

Social engineering of Active Directory

Social engineering of Active Directory is a common attack performed by red teamers to exploit one of the weakest points of an organization: the human element. Attackers utilize social engineering tactics, such as phishing, vishing and whaling, to gain access to internal networks, conduct ransomware attacks, steal proprietary information and more. For example, an attacker might send a well-crafted phishing e-mail to an organization that requires the users to log into a fake webpage, such as their e-mail, using their Active Directory credentials. The attacker then uses those credentials to access the employee's email and the internal network of the organization.

Social engineering prevention:

- The first step is user training. Train employees quarterly about common social engineering tactics and how they can spot them. Train employees on how to report suspicious social engineering events to the appropriate team. Training should include phishing/vishing campaigns and physical penetration tests to evaluate employee preparedness.
- Multi-factor authentication (MFA) should be implemented for all users and critical services, such as VPN access, e-mail, SharePoint, Azure AD etc. MFA adds another element of defense. For example, if an attacker calls a help desk line and successfully talks a help desk employee into resetting a user password, that attacker will still be met with an MFA request upon login.
- User access control, application whitelisting, anti-virus and intrusion prevention/detection systems are all additional measures that can protect against social engineering attacks. Preventing users from downloading suspicious files and/or executing those files as an administrator will help hinder attacks, as will detecting and reporting incidents to the appropriate team as they occur.

When all else fails, recover

If you've gone through a catastrophic AD event, you will remember the chaos it caused. Some very large organizations have undergone attacks against their AD and were forced to scrap it and start over. Consider both the physical and logical architecture, the delegations, the connections and trusts, all useless. Some organizations have had their directory taken down with ransomware and others have seen very important data walk out the door.

Once AD is compromised, don't trust it. If an attacker found a way in and compromised data, you can no longer trust the directory to be free from further intrusion. You must go through a painful rebuild or roll it back to a point where it could be trusted.

Whether you are looking at recovering attributes, objects, OU, schema or a restoration from a complete destruction, Quest Recovery Manager for AD makes this much less painful. Recovery Manager for Active Directory is a solution that feels like an insurance plan for your AD environment. Layering this with Change Auditor for AD, you can pinpoint changes to your AD environment at the object and attribute level, know what happened, who is impacted and what to roll back.

If you're dealing with a complete destruction of AD due to something like ransomware, Recovery Manager for Active Directory Disaster Recovery Edition automates and simplifies the recovery of objects and attributes, directories and servers, including state data and the operating system across the entire forest in the event of any disaster.

Conclusion

To summarize, we often hear about catastrophic attacks against companies, organizations and government agencies and even wonder how many happen that we don't hear about. Most of these enterprise-level attacks were either enabled by poor AD security or AD provided the mechanism to further the attack. Knowing your Active Directory and how to protect it is a constantly evolving task. So understanding the vulnerabilities as well as technology designed to protect is critical. To provide the best protection for any system, you must stay vigilant in your field and use all the right tools.

The offering

Quest Software, ICSynergy and One Identity have partnered to help identify these vulnerabilities, both in AD and in the enterprise by offering our customers a **Penetration Test Service**. This Pen Test can be as broad or as focused as you deem necessary and will provide insight into where your environment is secure and where some simple changes can significantly elevate your security posture.

A project with this type of reach requires a strong partnership between the provider and customer. Following our proven methodologies, we rely on the partnership between the project team, impacted teams and the business. We will engage all stakeholders as equal partners and co-author an achievable roadmap. We will leverage our process-driven integration model to co-develop an acceptable security posture while maintaining and improving usability. Our goal is to change the internal perception of AD security and PAM to accelerate the adoption across the organization.

For complete information on this service, contact your Quest, ICSynergy, or One Identity representative.

About One Identity

One Identity, a Quest Software business, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of the program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com.

About Quest

Quest provides software solutions for the rapidly changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid data centers, security threats and regulatory requirements. Our portfolio includes solutions for database management, data protection, unified endpoint management, identity and access management and Microsoft platform management.

About ICSynergy

ICSynergy is a North America-based Professional Services and Advisory firm focused on the hybrid Identity and Access Management security space. Our portfolio of services includes Cybersecurity Advisory, Privileged Identity Management, Pen Testing, Identity Governance and Access Management. In addition, we offer full-featured Managed Service Provider services for all of our practice areas.

Whitepaper_2020_HackingAD_RS_59069