Service Definition
AD Configuration Review and Password Audit

Introduction

Intertek NTA's AD Configuration & Password Auditing Service is designed to identify weak user passwords and misconfigurations in Active Directory demonstrating how they could be a security vulnerability on your network. The results of this service can be incorporated into your internal security training and used as a benchmark to determine the effectiveness of changes.

The service can be performed both remotely and internally depending on the level of service chosen. The 'Basic' password auditing service involves hash files being provided to Intertek NTA so analysis can be performed offsite. The 'Intermediate' and 'Advanced' services are performed to a greater depth and require an onsite presence. All password auditing is stored and performed offline on Intertek NTA's encrypted devices.

Scoping

A scoping conversation will be held prior to delivery to fully understand requirements and expectations, the size of the network to be tested and the type of systems that may be visible to the Internet. A recommended number of units/days will then be provided to enable requirements to be met.

Service Overview

Having been performing network security assessments for over 29 years', we have found that 98% of these have identified high risk vulnerabilities relating to password issues, which are normally associated with administrative users using weak passwords or passwords stored in clear text. Intertek NTA has developed the AD Configuration Review & Password Auditing Service to include a variety of tests that we believe is unique to the market and offers comprehensive value to our clients. These tests include:

Wordlist Audit

Intertek NTA's dedicated Research & Development team keep up to date with the latest wordlists used by attackers. This includes 2 billion weak and common passwords, passwords found on database leaks, passwords leaked online from phishing campaigns and common words and phrases.

Hybrid Audit

Advancement in technology allows modern devices to perform different variations of password attacks. Intertek NTA's password cracking services use extensive ranges of wordlists and are combined with our in-house rulesets, which are custom built and ever growing; currently containing 10 billion possible passwords.

LM Hash Review

Intertek NTA's experienced security testers can perform extensive analysis on users' password hashes that can indicate weaknesses on an organisation's network. Our detailed analysis will be able to report if weak hashes are used, if Domain Administrators are sharing passwords with Basic Users and if passwords are shared across multiple domains.

Service Definition
AD Configuration Review and Password Audit

Domain Admin Checks
During our analysis, we will perform checks to assess if domain administrators' passwords can be cracked. This is considered a critical issue in the vast number of penetration tests conducted by Intertek NTA's security testers.

Reversible Encryption Checks
Misconfiguration on a Domain Controller could lead to passwords being stored in cleartext. Intertek NTA will be able to identify accounts that are stored in cleartext and provide a remedial solution.

User Description Review
Passwords in user description tend to be overlooked. In recent years Intertek NTA has identified several tests where users have stored passwords in the user description, including administrative accounts. Intertek NTA will help identify accounts that have passwords stored in the user description field and validate them.

Privileged Group Checks
Intertek NTA will be able to identify privileged groups after enumerating systems in scope and review accounts that have been cracked. This allows you to identify privileged accounts that should be using more complex passwords or review the affected group and account.

Account Access on Servers and Workstations
Alongside the privileged group checks, Intertek NTA will be able to pinpoint accounts that are in the local administrative groups of a system and assess if they are using weak passwords. We will also be able to identify accounts in the privileged domain groups that are using weak passwords and report the affected system the groups or accounts currently reside on.

Shared Password Checks
Intertek NTA are able to identify basic user accounts sharing passwords with the domain administrator accounts. During an internal penetration test, this is considered a critical risk as it can be viewed as a privilege escalation vulnerability. Having obtained a basic user account, an attacker would be able to perform password spraying attack on the rest of the domain accounts and potentially obtain administrative accounts using the same password.

Password Registry Checks
Intertek NTA can identify passwords stored in the registry, with the associated account and application. From there we can then determine if the account is a domain account with privileged access and if further action needs to be taken to further secure the environment.

Shared Local Administrator Checks
Having shared local administrative accounts is a security risk because if one system gets compromised, all systems will be compromised as they are using the same local administrative credentials. Microsoft has released a tool called Local Administrator Password Solution (LAPS), which uniquely sets a password for administrative accounts on each system.

However, with Intertek NTA's experience in this field, we have identified several legacy administrative accounts that are left on systems and are still sharing the same passwords. We will be able to identify accounts that are sharing passwords with other systems by analysing and reviewing the hash of each system.

AD CS Checks
AD CS *(Active Directory Certificate Services)* is a server role that functions as Microsoft's public key infrastructure PKI implementation. It is integrated heavily with Active Directory and enables the issuing of certificates. AD CS Enterprise CAs issue certificates with settings defined by AD objects known as certificate templates. There are multiple misconfigurations that could allow privilege escalation or user credential theft. Intertek NTA will attempt to review these configurations to see if they are vulnerable. (Domain Escalations techniques ESC1 -10).

AD Group Mapping/Configuration/Analysis
Intertek NTA will analyse the Active Directory groups and memberships in the domain to assess potential privilege escalation routes, find privileged users that have rights to add members into groups, Principles with DCSync Rights, Map Domain Trusts, Path to Domain Admin from kerberoastable users for example.

Password Policy Review
Intertek NTA will analyse the password policy set at the Domain level and local servers/end user devices in accordance with best practice and recommendations from NCSC/CIS/NIST. Specific settings such as minimum password length, account lockout, password complexity and reset account lockout counter.

Fine Grain Password Policy Review
Additionally, to the above password policy audit Intertek NTA will review any fine-grained password policies set for administrators or privileged users settings for minimum password length, account lockout, password complexity and reset account lockout counter.

AD Configuration Review & Password Analysis Report
Intertek NTA's AD Configuration Review & Password Audit report can be tailored to your specific needs. However, as standard you will be provided with a spreadsheet that lists those accounts using weak passwords, highlighting any domain administrator accounts.

The 'Intermediate' and Advanced' options include additional detail identifying systems that are storing passwords in cleartext, having additional accounts or a legacy local account that could be sharing passwords with another system.

Deliverables
Intertek NTA's AD Configuration Review & Password Audit report can be tailored to your specific needs. However, as standard you will be provided with a spreadsheet that lists those accounts using weak passwords, highlighting any domain administrator accounts.

The 'Intermediate' and Advanced' options include additional detail identifying systems that are storing passwords in cleartext, having additional accounts or a legacy local account that could be sharing passwords with another system.

Service Definition
AD Configuration Review and Password Audit

Service Management
You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

Intertek NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, Int NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling the test, ensuring reports are sent out in a timely manner, scheduling follow up tests and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

Ordering and Invoicing Process
Once the scope of work and number of units/days required has been agreed between the customer and Inter NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.