SYSLIFTERS

Demo-Report: Active Directory

Pentest für **Security Maximale GmbH**
2022-09-12
v 1.0

Kontakt:
Aron Molnar
+43 660 923 40 60
aron@syslifters.com

Inhalt

Management Summary

Im Zuge des Pentests der internen Infrastruktur konnte die Windows Active Directory Domain über mehrere Wege vollständig kompromittiert werden. Ein Angreifer mit den Standardberechtigungen eines Mitarbeiters könnte damit Zugriff auf alle in der Windows-Domäne verwalteten Ressourcen (inkl. E-Mails, Server, PCs, Dateien, etc). erlangen.

Diese Rechteerhöhung gelang etwa über fehlerhafte Konfigurationen des Active Directory (fehlerhafte Zugriffskontrollen auf Zertifikatsvorlagen, unsichere dynamische DNS-Updates, Unconstrained Delegation). Eine Rechteerhöhung war außerdem möglich, da Zugangsdaten von lokalen Administratoren in der Benutzerbeschreibung mehrerer Benutzer, sowie in den Einstellungen von Gruppenrichtlinien auslesbar waren.

Mehrere Dutzend Systeme konnten über kritische Schwachstellen aufgrund fehlender Updates vollständig kompromittiert werden. Wir empfehlen dringend, die regelmäßige Installation von Updates im Zuge eines Patch-Management-Prozesses sicherzustellen.

Hier ist der Bericht. Was jetzt?

Es ist uns sehr wichtig, dass ihr mit unserem Bericht arbeitet und Verbesserungsmaßnahmen daraus ableitet. Deshalb testen wir für euch behobene Schwachstellen kostenlos nach, wenn sie innerhalb von acht Wochen behoben werden!

In diesem Assessment haben wir Schwachstellen mit der Kritikalität `Critical` und `High` gefunden. Wir empfehlen, diese Schwachstellen vorrangig zu beheben.

Schwachstellen mit weniger komplexen Gegenmaßnahmen und Risiko `Medium` und darunter sollten nach unserer Empfehlung nach Aufwand priorisiert behoben werden. Alle anderen Schwachstellen sollten im Rahmen eines kontinuierlichen Verbesserungsprozesses adressiert werden.

Bitte stellt sicher, alle im Zuge des Pentests bereitgestellten Benutzer und Ressourcen zu deprovisionieren, sobald sie nicht mehr benötigt werden.

Scope und Dauer

Für diesen Pentest haben wir Zugriff auf das interne Netzwerk der Security Maximale GmbH am Standort Stephansplatz 1, 1010 Wien erhalten. Es wurden zwei Microsoft Windows Notebooks (Hardware) und drei Benutzerkonten zur Verfügung gestellt. Einer der Benutzer hatte lokale Admin-Rechte auf einem bereitgestellten Notebook.

Der Scope des Penetration-Tests umfasste:

- Active Directory-Infrastruktur
- Notebooks mit Microsoft Windows
- Windows- und UNIX-Server
- 10.17.1.0/24
- 10.17.5.0/24
- 10.17.10.0/24
- 10.17.11.0/24
- 10.20.1.0/24
- 10.20.2.0/24
- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.10.0/24

Der Penetration-Test erfolgte nach einem Time-Box-Ansatz und umfasste 10 Personentage.

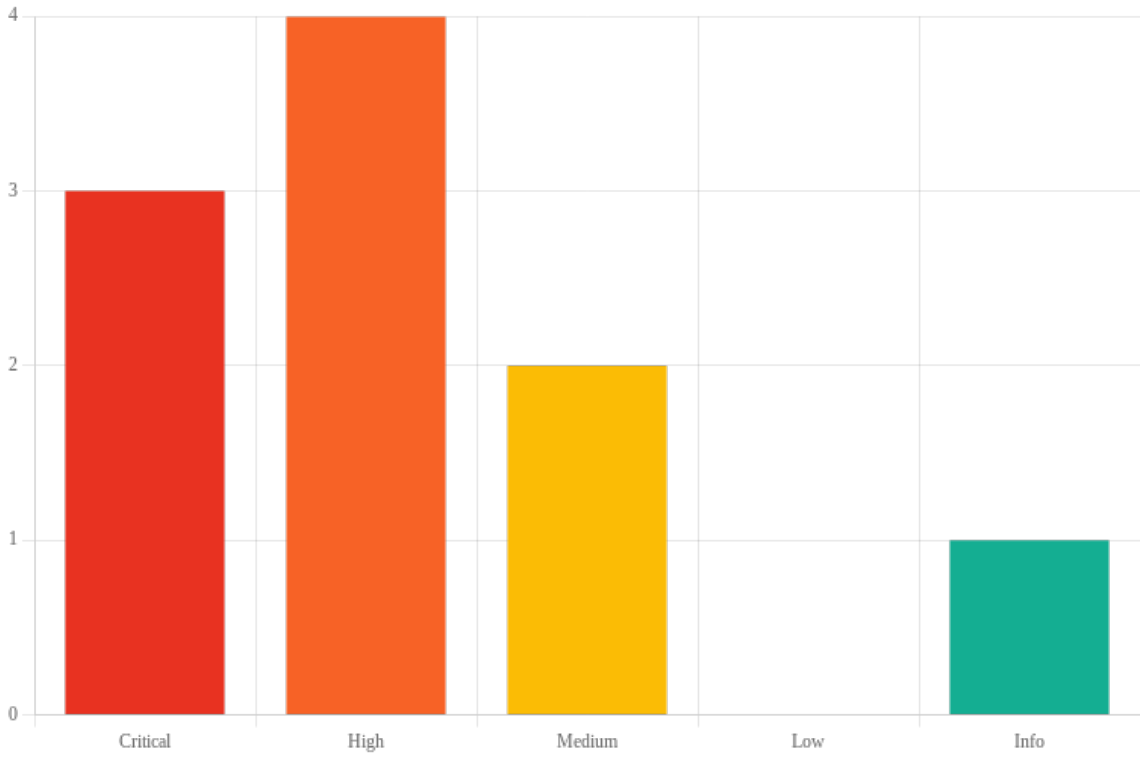
Folgende Windows Client-Rechner und Benutzer wurden uns bereitgestellt:

- Client-Rechner: PENTEST-CLIENT01
- Client-Rechner: PENTEST-CLIENT02
- Localer Benutzer: pentest_local_admin
- AD Benutzer: PENTEST01
- AD Benutzer: PENTEST02

Wir empfehlen, alle Benutzerkonten und Ressourcen zu deprovisionieren, sobald sie nicht mehr benötigt werden.

Schwachstellenübersicht

Im Rahmen dieses Penetration Tests wurden **3 Critical** , **4 High** , **2 Medium** und **1 Info** Schwachstellen identifiziert:



Verteilung der gefundenen Schwachstellen

Eine tabellarische Übersicht aller gefundenen Schwachstellen:

Schwachstelle	Kritikalität
Unsichere Zertifikatsvorlagen	Critical
Schwachstellen in veralteter Software	Critical
Unsichere DNS-Einstellungen ermöglichen MitM-Angriffe	Critical
Zugangsdaten in Group Policy Preferences	High
Zugangsdaten in Active Directory-Feldern	High
Unconstrained Delegation für Dienstkonten	High
Benutzerkonten anfällig für Kerberoasting	High
Schwache Anforderungen an die Passwortkomplexität	Medium
Netzwerkzugriff aufgrund fehlender NAC-Lösung	Medium

Schwachstelle	Kritikalität
Windows Active Directory Audit	Info

Eine Auflistung aller Schwachstellen inklusive Kurzbeschreibung:

1. Unsichere Zertifikatsvorlagen (Critical: 9.9)
Betrifft: Zertifikatsvorlage "SmartcardUsers" der Certificate Authority "ca01.lab.local"

Wir konnten im Zuge der Prüfung verwundbare Zertifikatsvorlagen identifizieren, die von Active Directory Certificate Services (AD CS) als Basis für die Ausstellung von Zertifikaten herangezogen wurden. Ein authentifizierter Angreifer kann über AD CS Zertifikate ausstellen, die aufgrund von Fehleinstellungen auf einen beliebigen Benutzer lauten und zur Authentifizierung im Active Directory verwendet werden können. Ein Angreifer könnte dadurch die Rechte eines Domänenadministrators erlangen und die gesamte Domäne übernehmen.

2. Schwachstellen in veralteter Software (Critical: 9.8 | Teilweise Behoben)
Betrifft: Systeme im internen Netzwerk

Wir konnten mehrere Softwarepakete identifizieren, die zum Zeitpunkt der Prüfung nicht mehr auf dem neuesten Stand waren und bekannte Schwachstellen beinhalteten. Darunter waren Software-Versionen mit kritischen Schwachstellen, die die vollständige Kompromittierung der Systeme erlauben, etwa MS08-067 (z. B. genutzt vom Conficker-Wurm aus dem Jahr 2008), Shellshock, MS17-010 (z. B. genutzt von der Ransomware WannaCry), BlueKeep und andere.

Von **437 gescannten Systemen** hatten **15 Systeme** zumindest eine **kritische** Schwachstelle und **38 Systeme** zumindest eine **hohe** Schwachstelle. Zudem waren 132 Systeme von Schwachstellen mit mittlerem, sowie 289 Systeme von Schwachstellen mit niedrigem Risiko betroffen.
Eine genaue Übersicht sämtlicher Schwachstellen ist im beigelegten Bericht des Schwachstellenscans von Tenable Nessus zu finden.

3. Unsichere DNS-Einstellungen ermöglichen MitM-Angriffe (Critical: 9.0 | Behoben)
Betrifft: Active Directory DNS Zonen

Das ADIDNS war zum Zeitpunkt der Prüfung so konfiguriert, dass unauthentifizierte Benutzer DNS-Einträge manipulieren konnten. Dies ermöglicht es Angreifern, Netzwerkverkehr umzuleiten, zu lesen und zu verändern.

Bei einem erfolgreichen Angriff könnte ein Angreifer an Anmeldeinformationen gelangen, um Code auf fremden Systemen auszuführen oder sich lateral im Netzwerk zu bewegen.

4. Zugangsdaten in Group Policy Preferences (High: 8.8 | Behoben)

Wir konnten Zugangsdaten von lokalen Administratoren in Group Policy Preferences (GPP) identifizieren. GPPs werden im SYSVOL-Verzeichnis am Domänencontroller abgelegt, auf welches authentifizierte Benutzer standardmäßig Lesezugriff haben. Die Passwörter sind verschlüsselt, jedoch ist der von Microsoft verwendete Schlüssel öffentlich bekannt. Jeder Domänenbenutzer kann daher verfügbare GPPs einsehen und die darin gespeicherten Passwörter entschlüsseln. Ein Angreifer könnte dadurch seine Rechte in der Domäne ausweiten.

5. Zugangsdaten in Active Directory-Feldern (High: 8.8 | Behoben)

Wir konnten im Zuge der Prüfung Passwörter von Benutzern identifizieren, die im Feld "Beschreibung" von Active Directory-Benutzerobjekten hinterlegt waren. Diese konnten erfolgreich für eine Anmeldung verwendet werden. Das Feld ist für alle authentifizierten Active Directory-Benutzer lesbar.

6. Unconstrained Delegation für Dienstkonten (High: 8.5)
Betrifft: Dienstkonten IIS01-03

Wir identifizierten drei Dienstkonten (IIS01-03) in der Active Directory-Domäne, für welche unsichere Kerberos Unconstrained Delegation konfiguriert waren. Angreifer, die eines dieser Dienstkonten erfolgreich kompromittieren, können auf zwischengespeicherte Authentifizierungstickets zugreifen. Auf den Domain Controllern ist zudem der Print Spooler Service aktiv. Dadurch kann ein Angreifer aktiv eine Authentifizierung der Domain Controller anstoßen, was diese Schwachstelle zusätzlich verschärft. Ein Angreifer könnte dadurch die Rechte eines Domänenadministrators erlangen.
Wir konnten die Schwachstelle nicht erfolgreich ausnutzen, da wir keines der drei Dienstkonten erfolgreich übernehmen konnten.

7. Benutzerkonten anfällig für Kerberoasting (High: 8.4 | Teilweise Behoben)
Betrifft: Service Accounts im Active Directory

Wir identifizierten drei hoch privilegierte Dienstkonten (insgesamt: 4), die anfällig für Kerberoasting waren. Niedrig privilegierte Angreifer können Service-Tickets dieser Dienstkonten anfordern und das jeweilige Klartext-Passwort im Zuge eines Offline-Brute-Force-Angriff erraten. Bei Offline-Brute-Force-Angriffen können Passwörter erheblich schneller geknackt werden, als über das Netzwerk. Im Zuge der Prüfung konnten wir zwei Klartext-Passwörter erfolgreich knacken.

8. Schwache Anforderungen an die Passwortkomplexität (Medium: 5.9)

Zum Zeitpunkt der Prüfung waren schwache Kennwortrichtlinien in der Active Directory-Umgebung konfiguriert. Die erforderliche Passwortlänge betrug lediglich sieben Zeichen und es wurden keine Komplexitätsanforderungen erzwungen. Schwache Passwörter können in der Regel durch Brute-Force Angriffe in kurzer Zeit erraten werden. Bei erfolgreichem Erraten des Passworts eines privilegierten Benutzerkontos, könnte ein Angreifer die gesamte Domäne übernehmen.

9. Netzwerkzugriff aufgrund fehlender NAC-Lösung (Medium: 4.3 | Akzeptiert)
Betrifft: Layer 2 Netzwerk/Netzwerkports am Standort Stephansplatz 1, 1010 Wien

Wir konnten uns im Zuge der Prüfung Zugang zum Unternehmensnetzwerk aufgrund einer fehlenden Network Access Control (NAC)-Lösung verschaffen. NAC ist eine Maßnahme, die sicherstellt, dass nur vertrauenswürdige Geräte eine Verbindung zum Unternehmensnetzwerk herstellen dürfen und dass diese alle Anforderungen des Netzwerks erfüllen, bevor sie Zugang erhalten. Nicht vertrauenswürdige und nicht autorisierte Geräte werden dadurch vom Netzwerk ferngehalten. Wenn jedoch keine NAC-Lösung im Unternehmen etabliert ist, können Angreifer Computer, Computerzubehör oder Netzwerkhardware im Netzwerk platzieren, die als Ausgangspunkt für den Zugriff auf interne Ressourcen genutzt werden können.

10. Windows Active Directory Audit (Info: 0.0)
Betrifft: Active Directory-Benutzerobjekte

Im Rahmen des Penetration-Tests wurden die in Active Directory gespeicherten User- und Computer-Objekte analysiert und verschiedene Metriken ausgewertet.

Schwachstellendetails

1. Unsichere Zertifikatsvorlagen

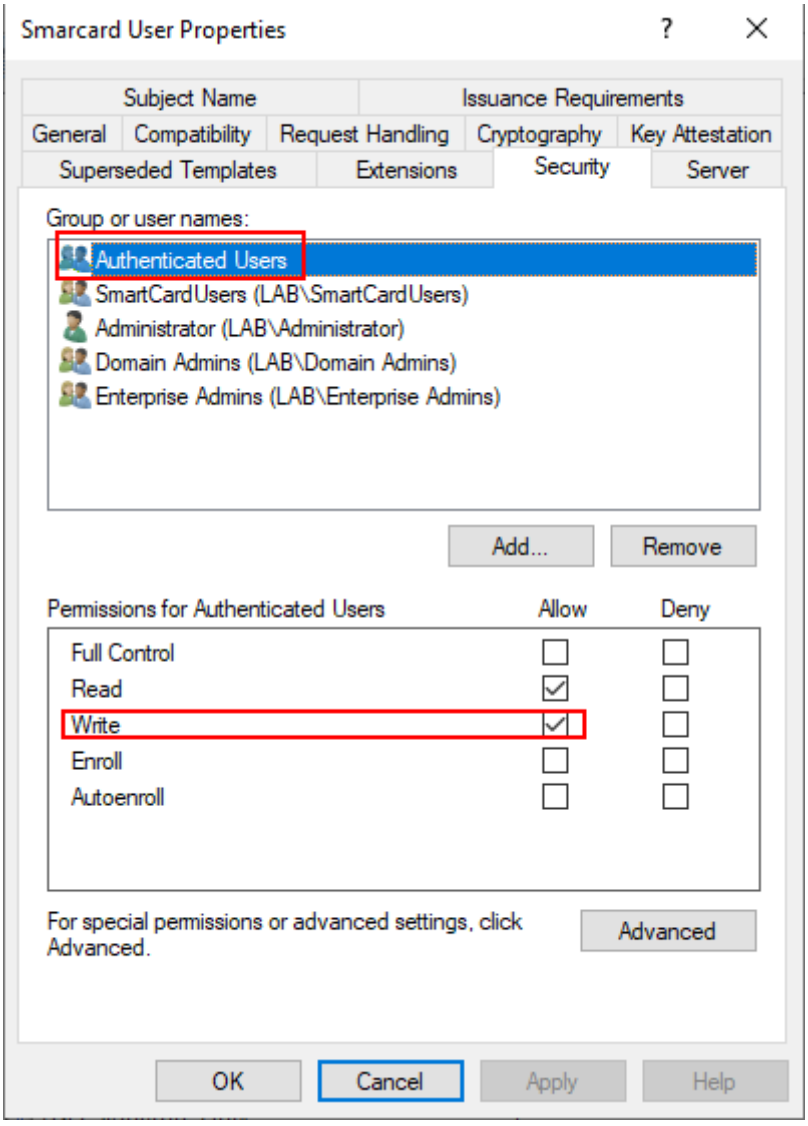
Kritikalität: Critical
CVSS-Score: 9.9
Betrifft: Zertifikatsvorlage "SmartcardUsers" der Certificate Authority "ca01.lab.local"
Empfehlung: Alle Enterprise-CAs und Zertifikatsvorlagen sollten auf unsichere Einstellungen und Berechtigungen überprüft werden.

Überblick

Wir konnten im Zuge der Prüfung verwundbare Zertifikatsvorlagen identifizieren, die von Active Directory Certificate Services (AD CS) als Basis für die Ausstellung von Zertifikaten herangezogen wurden. Ein authentifizierter Angreifer kann über AD CS Zertifikate ausstellen, die aufgrund von Fehleinstellungen auf einen beliebigen Benutzer lauten und zur Authentifizierung im Active Directory verwendet werden können. Ein Angreifer könnte dadurch die Rechte eines Domänenadministrators erlangen und die gesamte Domäne übernehmen.

Beschreibung

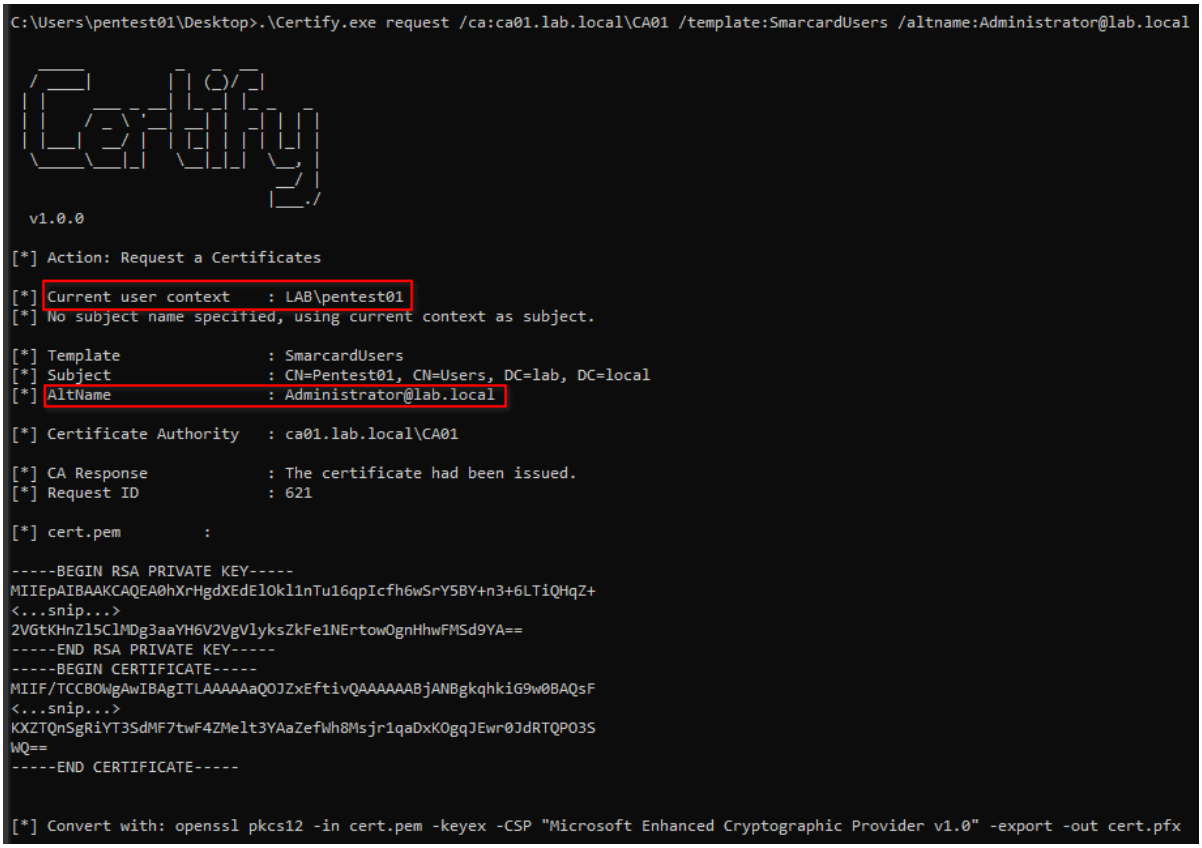
Im Zuge der Prüfung war es uns möglich, die Zertifikatsvorlage `SmartcardUsers` zu bearbeiten. Die Berechtigungen sind im folgenden Screenshot ersichtlich.



Berechtigungen von authentifizierten Benutzern für die Zertifikatsvorlage SmartcardUsers

Zwar konnten zum Zeitpunkt der Prüfung angemeldete Benutzer keine neuen Zertifikate ausstellen, jedoch konnten wir dies wegen der konfigurierten Schreibberechtigungen ändern. Zudem konnten wir die Einstellung `USER_INTERACTION_REQUIRED` deaktivieren, sodass keine Benutzerbenachrichtigung bei Ausstellung eines Zertifikats erfolgt, sowie die Verwendung des SAN-Feldes erlauben.

Da die Zertifikatsvorlage Client-Authentifizierungen erlaubte, mussten wir diese Einstellung nicht anpassen. Somit konnten wir die Zertifikatsvorlage nutzen, um uns mit dem Benutzer `PENTEST01` ein Zertifikat mit den SAN `Administrator` auszustellen.



Ausstellen eines Zertifikats von der modifizierten Zertifikatsvorlage

Um das Zertifikat für eine Anmeldung verwenden zu können, haben wir mit dem Kerberos-Client `Rubeus` ein Kerberos Ticket-Granting-Ticket für den Benutzer `Administrator` ausgestellt. Das konnten wir schließlich für weitere Authentifizierungen verwenden.

```
C:\Users\pentest01\Desktop>.\Rubeus.exe asktgt /user:Administrator /certificate:cert.pfx /ptt

  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.0.0

[*] Action: Ask TGT

[*] Using PKINIT with etype rc4_hmac and subject: CN=Pentest01, CN=Users, DC=lab, DC=local
[*] Building AS-REQ (w/ PKINIT preauth) for: 'lab.local\Administrator'
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFujCCBbagAwIBBaEDAgEWooIE0zCCBM9hggTLMIIEx6ADAgEFoQsbCUxBQi5MT0NBTKIeMBygAwIB
      <...snip...>
      MBygAwIBAqEVMBMbBmtyYnRndBsJbGFiLmxvY2Fs
[+] Ticket successfully imported!

  ServiceName              :  krbtgt/lab.local
  ServiceRealm             :  LAB.LOCAL
  UserName                 :  Administrator
  UserRealm                :  LAB.LOCAL
  StartTime                :  21/04/2022 12:49:44
  EndTime                  :  21/04/2022 22:49:44
  RenewTill                :  28/04/2022 12:49:44
  Flags                    :  name_canonicalize, pre_authent, initial, renewable, forwardable
  KeyType                  :  rc4_hmac
```

Ausstellung eines Kerberos TGT mittels Zertifikat

Dadurch war es uns möglich, uns gegenüber dem Domänencontroller als Domänenadministrator zu authentifizieren und die gesamte Domäne zu übernehmen.

Active Directory Certificate Services (AD CS) ist eine in Windows Server integrierte Serverrolle und bietet verschiedene Services zur Erstellung und Verwaltung einer data Key Infrastruktur (PKI). Zertifikate werden zur Verschlüsselung (z.B. des Dateisystems), Signierung von Nachrichten (z.B. Code Signing) oder zur Authentifizierung (z.B. dem Active Directory gegenüber) verwendet. Es enthält unterschiedliche Felder, wie z.B.

- Subject: Inhaber des Zertifikats
- data Key: Öffentliche Schlüssel, der den Eigentümer mit einem separat gespeicherten privaten Schlüssel verknüpft
- NotBefore and NotAfter: Legen die Gültigkeitsdauer des Zertifikats fest
- Serial Number: Eindeutige Kennung des Zertifikats
- Issuer: Gibt die Zertifizierungsstelle an, die das Zertifikat ausgestellt hat
- SubjectAlternativeName (SAN): Definiert alternative Namen des Inhabers
- Basic Constraints: Gibt Beschränkungen bei der Verwendungen des Zertifikats bekannt
- Extended Key Usages (EKUs): Beinhaltet Objektbezeichner (OIDs), die beschreiben, wie das Zertifikat verwendet werden soll/kann (z.B. Code-Signing, Server-Authentifizierung, Client-Authentifizierung, etc.)

- Signature Algorithm: Gibt den Algorithmus an, der zum Signieren des Zertifikats verwendet wurde.
- Signature: Digitale Signatur vom Zertifikat, die mit dem privaten Schlüssel des Issuers (z.B. CA) erzeugt wurde

In der Rolle AD CS werden Zertifikate über einen Enrollment-Prozess ausgestellt. Clients stoßen diesen Prozess an, indem sie zunächst verfügbare Enterprise CAs im Active Directory identifizieren. Die Clients generieren dann ein asymmetrisches Schlüsselpaar. Der öffentliche Schlüssel, das Subject und der Name einer Zertifikatsvorlage werden anschließend in einer CSR (Certificate Signing Request) Nachricht zusammengefasst und mit dem privaten Schlüssel signiert. Die CSR-Nachricht wird dann vom Client an einen Enterprise CA Server gesendet. Sofern der Client Zertifikate anfordern darf, generiert die CA auf Basis der gewünschten Zertifikatsvorlage und unter Verwendung der in der CSR-Nachricht bereitgestellten Informationen ein neues Zertifikat.

Zertifikatsvorlagen werden von der CA als Basis für neue Zertifikate verwendet. Sie legen vordefinierte Zertifikatseinstellungen fest, wie z.B. wie lange ein Zertifikat gültig ist, wofür das Zertifikat verwendet werden darf oder wer Zertifikate anfordern darf. Nachdem ein neues Zertifikat ausgestellt wurde, wird es im letzten Schritt von der CA mit ihrem privaten Schlüssel signiert und dem Client übermittelt. Der Client kann das Zertifikat schließlich für den vorgesehenen Zweck, der durch die EKUs bestimmt wird, verwenden.

Empfehlung

- Die Schreibberechtigungen für die Zertifikatsvorlage `SmartcardUsers` sollten entfernt werden. Folgende Einstellungen beinhalten Schreibberechtigungen:
  - `FullControl`
  - `WriteDacl`
  - `WriteOwner`
  - `WriteProperty`
- Alle CAs sollten auf unsichere Einstellungen und Berechtigungen überprüft werden:
  - Nach Möglichkeit sollte die Einstellung EDITF_ATTRIBUTESUBJECTALTNAME2 auf allen CAs deaktiviert werden. Alternativ sollte eine Manager-Genehmigung für jede Zertifikatsvorlage, die eine Domänenauthentifizierung ermöglicht, konfiguriert werden.
  - Es sollte eingeschränkt werden, wer als Enrollment Agent fungieren darf und für welche Benutzer/Zertifikatsvorlagen diese Agents Zertifikate anfordern dürfen.
  - Berechtigungen von Benutzern/Gruppen auf CA-Server sollten so weit wie möglich eingeschränkt werden.
- Alle Zertifikatsvorlagen sollten auf unsichere Einstellungen und Berechtigungen überprüft werden:
  - Wenn die Ausstellung von Zertifikaten keine SAN-Spezifikation erfordert, sollte die Einstellung von der Vorlage entfernt werden.

    - Sofern die Spezifikation von SubjectAlternativeNames erforderlich ist, sollte die entsprechende Vorlage die Genehmigung durch einen Manager aktivieren.
    - CSRs sollten nach Möglichkeit von bestehenden autorisierten Zertifikaten signiert werden müssen.
    - Die Anforderung neuer Zertifikate sollte nur ausgewählten Benutzern/Gruppen möglich sein.
    - Es sollte darauf geachtet werden, dass Benutzer keine Schreibberechtigungen auf Zertifikatsvorlagen besitzen.
    - Es sollten in der Vorlage nur notwendige EKUs angegeben werden. Vorlagen mit umfangreichen EKUs sollten auf privilegierte Benutzer/Gruppen beschränkt werden.
- CA-Server sollten als Tier 0-Ressourcen angesehen und daher wie ein Domänencontroller geschützt werden.
- AD CS HTTP Endpunkte sollten deaktiviert werden, sofern sie nicht benötigt werden. Andernfalls sollte HTTPS für den Zugriff auf die Endpunkte erzwungen und nach Möglichkeit die Verwendung von NTLM beschränkt werden. Zur Einschränkung von NTLM-Relay Angriffen sollte zudem Extended Protection for Authentication (EPA) aktiviert werden.

2. Schwachstellen in veralteter Software

Remediation Status: Teilweise Behoben
Kritikalität: Critical
CVSS-Score: 9.8
Betrifft: Systeme im internen Netzwerk
Empfehlung: Software sollte stets auf dem neuesten Stand gehalten werden. Wir empfehlen dazu, einen Patch-Management-Prozess zu implementieren, der regelmäßige Updates sicherstellt.

Überblick

Wir konnten mehrere Softwarepakete identifizieren, die zum Zeitpunkt der Prüfung nicht mehr auf dem neuesten Stand waren und bekannte Schwachstellen beinhalteten. Darunter waren Software-Versionen mit kritischen Schwachstellen, die die vollständige Kompromittierung der Systeme erlauben, etwa MS08-067 (z. B. genutzt vom Conficker-Wurm aus dem Jahr 2008), Shellshock, MS17-010 (z. B. genutzt von der Ransomware WannaCry), BlueKeep und andere.

Von **437 gescannten Systemen** hatten **15 Systeme** zumindest eine **kritische** Schwachstelle und **38 Systeme** zumindest eine **hohe** Schwachstelle. Zudem waren 132 Systeme von Schwachstellen mit mittlerem, sowie 289 Systeme von Schwachstellen mit niedrigem Risiko betroffen.
Eine genaue Übersicht sämtlicher Schwachstellen ist im beigelegten Bericht des Schwachstellenscans von Tenable Nessus zu finden.

Anmerkungen zu Behebungsstatus

Der Nachtest zeigte, dass Systeme mit kritischen Schwachstellen (BlueKeep, MS17-010, MS08-067, Shellshock) gepatcht wurden, sodass diese nicht mehr verwundbar sind.

Es befinden sich jedoch noch einige Systeme mit nicht mehr unterstützen Versionen im Betrieb.

Beschreibung

Im Zuge der Prüfung haben wir einen automatisierten, authentifizierten Schwachstellenscan mit Tenable Nessus durchgeführt. Eine genaue Übersicht sämtlicher Schwachstellen ist im beigelegten Bericht des Schwachstellenscans von Tenable Nessus zu finden. Die Schwachstellen mit den höchsten Risiken listen wir in der folgenden Übersicht auf:

Microsoft RDP RCE (CVE-2019-0708) (BlueKeep)

- 10.17.1.80 (tcp/3389/msrdp)
- 10.17.1.209 (tcp/3389/msrdp)
- 10.17.1.212 (tcp/3389/msrdp)
- 10.17.1.219 (tcp/3389/msrdp)

Veraltete Microsoft SQL-Server

Host	Microsoft SQL Server Version
10.17.1.34 (tcp/1433/mssql)	8.0.2039.0
10.17.1.40 (tcp/1433/mssql)	12.0.5000.0
10.17.1.44 (tcp/62084/mssql)	13.0.4001.0

Veraltete Windows-Versionen

- Microsoft Windows Server 2003 Service Pack 2
- Windows XP for Embedded Systems
- Microsoft Windows Server 2008 R2 Standard Service Pack 1
- Microsoft Windows Server 2008 R2 Foundation Service Pack 1
- Microsoft Windows 7 Professional

Wir konnten **62 Systeme** mit veralteten Windows-Betriebssystem-Versionen identifizieren. Die genaue Übersicht der Systeme ist im beigelegten Bericht des Schwachstellenscans zu finden.

MS17-010: ETERNALBLUE/ETERNALCHAMPION/ETERNALROMANCE/ ETERNALSYNERGY/WannaCry/EternalRocks/Petya

- 10.17.1.25 (tcp/445/cifs)
- 10.17.1.39 (tcp/445/cifs)
- 10.17.10.122 (tcp/445/cifs)
- 10.17.11.137 (tcp/445/cifs)

MS08-067

- 10.17.11.139 (tcp/445/cifs)

GNU Bash Environment Variable Handling Code Injection (Shellshock)

- 10.20.1.245 (tcp/80/www)
- 10.20.1.246 (tcp/80/www)

Empfehlung

- Veraltete Software mit kritischen und hohen Schwachstellen sollten so bald wie möglich aktualisiert werden.
- Systeme und Software sollten stets auf dem neuesten Stand gehalten werden.
- Wir empfehlen dazu, einen Patch-Management-Prozess zu implementieren, der regelmäßige Updates sicherstellt.
- Wir empfehlen je nach Anwendungsfall meist auch den Einsatz automatischer Update-Mechanismen.

3. Unsichere DNS-Einstellungen ermöglichen MitM-Angriffe

Remediation Status: Behoben
Kritikalität: Critical
CVSS-Score: 9.0
Betrifft: Active Directory DNS Zonen
Empfehlung: DNS-Zonen sollten ausschließlich sichere dynamische DNS-Updates erlauben. Zugriffsrechte für DNS-Zonen sollten eingeschränkt werden, um ADIDNS-Angriffe zu erschweren.

Überblick

Das ADIDNS war zum Zeitpunkt der Prüfung so konfiguriert, dass unauthentifizierte Benutzer DNS-Einträge manipulieren konnten. Dies ermöglicht es Angreifern, Netzwerkverkehr umzuleiten, zu lesen und zu verändern.

Bei einem erfolgreichen Angriff könnte ein Angreifer an Anmeldeinformationen gelangen, um Code auf fremden Systemen auszuführen oder sich lateral im Netzwerk zu bewegen.

Anmerkungen zu Behebungsstatus

Alle empfohlenen Maßnahmen wurden umgesetzt.

Beschreibung

Die Active Directory Domain Services (AD DS) ermöglichen es, DNS-Informationen im Active Directory zu verwalten. Dies wird als Active Directory-integrated DNS (ADIDNS) bezeichnet.

Zum Zeitpunkt der Prüfung waren "unsichere dynamische Updates" konfiguriert. Damit war es als unauthentifizierter Benutzer möglich, vorhandene DNS-Einträge zu modifizieren, sowie neue DNS-Einträge zu erstellen. Angreifer können dies ausnutzen, um Datenverkehr umzuleiten und so in eine MitM-Position zu gelangen.

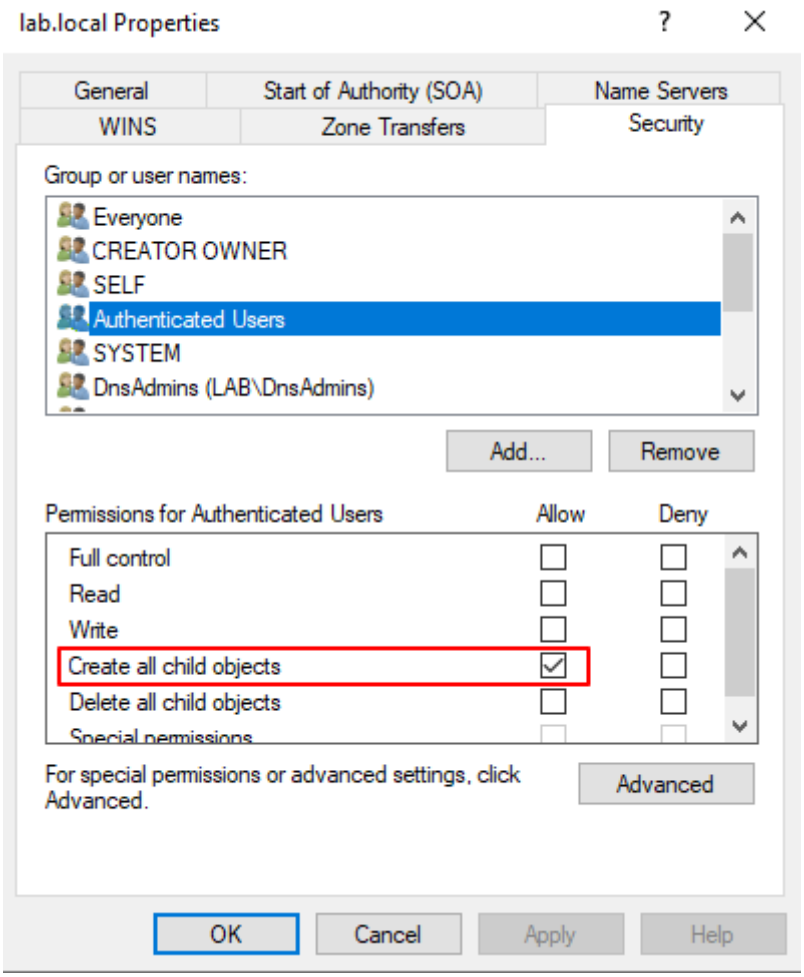
ADIDNS-Zonen können von remote über dynamische Updates oder unter Verwendung von LDAP geändert werden. Das DNS Dynamic Update Protocol ist ein DNS-spezifisches Protokoll, das für die Aktualisierung von DNS-Zonen entwickelt wurde. Im Active Directory werden dynamische Updates hauptsächlich von Computerkonten genutzt, um ihre eigenen DNS-Einträge hinzuzufügen und zu aktualisieren.

Bei der Anwendung von "sicheren dynamischen Updates" können standardmäßig neue DNS-Einträge hinzugefügt werden, bestehende Einträge jedoch nicht modifiziert werden.

Bei "unsicheren dynamischen Updates" ist auch die Modifikation möglich. Dies bietet Angreifern eine erheblich größere Angriffsfläche.

Auch die Erstellung neuer DNS-Einträge stellt ein erhebliches Risiko dar. Wenn nämlich ein Hostname im DNS nicht existiert, lösen Windows-Clients die Namen standardmäßig zusätzlich über LLMNR und NBT-NS auf. Ein Angreifer könnte durch das Setzen eines neuen DNS-Eintrages die Übersetzung des Namens auf eine IP-Adresse über DNS kontrollieren, oder LLMNR- und NBT-NS-Antworten fälschen.
Das erlaubt dem Angreifer, den Netzwerkverkehr zu sich umzuleiten und etwa an Anmeldeinformationen zu gelangen.

Das Hinzufügen neuer DNS-Einträge ist wegen der standardmäßig gesetzten Berechtigung "Create all child objects" für authentifizierte Benutzer möglich.



Berechtigungen angemeldeter Benutzer für das Erstellen neuer DNS Einträge

Empfehlung

- Schränkt die Zugriffsberechtigungen für DNS-Zonen ein, um zu verhindern, dass authentifizierte Benutzer neue DNS-Einträge erstellen können.

- Stellt sicher, dass ausschließlich sichere dynamische DNS-Updates erlaubt sind.
- Verwendet ein dediziertes Benutzerkonto für dynamische DNS-Updates per DHCP.
- Für eine weitere Absicherung, erstellt in allen Zonen einen Wildcard- (`*`), sowie einen `wpad`-Record (z. B. als TXT-Record).
- Mail-Clients sollten Bilder zumindest für externe Absender nicht automatisch nachladen.

Weiterführende Informationen

- https://www.netspi.com/blog/technical/network-penetration-testing/exploiting-adidns/
- https://www.netspi.com/blog/technical/network-penetration-testing/adidns-revisited/
- https://docs.microsoft.com/de-de/troubleshoot/windows-server/networking/configure-dns-dynamic-updates-windows-server-2003

4. Zugangsdaten in Group Policy Preferences

Remediation Status: Behoben
Kritikalität: High
CVSS-Score: 8.8
Empfehlung: Die Passwörter sollten aus den Konfigurationsdateien entfernt und für die betroffenen Benutzerkonten ("LocalAdministrator") geändert werden.

Überblick

Wir konnten Zugangsdaten von lokalen Administratoren in Group Policy Preferences (GPP) identifizieren. GPPs werden im SYSVOL-Verzeichnis am Domänencontroller abgelegt, auf welches authentifizierte Benutzer standardmäßig Lesezugriff haben. Die Passwörter sind verschlüsselt, jedoch ist der von Microsoft verwendete Schlüssel öffentlich bekannt. Jeder Domänenbenutzer kann daher verfügbare GPPs einsehen und die darin gespeicherten Passwörter entschlüsseln. Ein Angreifer könnte dadurch seine Rechte in der Domäne ausweiten.

Anmerkungen zu Behebungsstatus

Im Zuge des Nachtests wurde festgestellt, dass alle identifizierten Passwörter aus den Gruppenrichtlinien entfernt wurden. Die Passwörter der darin enthaltenen Benutzer wurden geändert.

Dieses Finding wurde damit erfolgreich behoben.

Beschreibung

Die Passwörter der folgenden Benutzerkonten wurden entschlüsselt und sind somit als kompromittiert zu betrachten. Die Konten waren Teil einer privilegierten Gruppe und besaßen die Berechtigungen lokaler Administratoren.

- Group Policy "GPAccounting" - Benutzer "LocalAdministrator"
- Group Policy "GPMarketing" - Benutzer "LocalAdministrator"

Group Policies ermöglichen die zentrale Verwaltung und Konfiguration von Betriebssystemen, Anwendungen und Benutzereinstellungen in einer Active Directory Umgebung. Als Group Policy Object (GPO) wird eine Sammlung von Group Policy Einstellungen bezeichnet. Ein GPO ist ein logisches Objekt, das aus zwei Komponenten besteht: einem Group Policy Container und einem Group Policy Template. Das Container-Objekt ist in der Domänenpartition von Active Directory gespeichert. Das Template-Objekt enthält eine Sammlung von Dateien und Ordnern, die auf dem Systemvolume (SYSVOL) jedes Domänencontrollers in der Domäne gespeichert ist.

Jedes GPO kann zwei Klassen von Konfigurationen enthalten: Benutzer- und / oder Computereinstellungen. Einstellungen betreffend Computerkonfiguration wirken sich auf Computer als Ganzes aus, unabhängig vom angemeldeten Benutzer. Einstellungen betreffend Benutzerkonfiguration wirken sich hingegen auf den aktuell angemeldeten Benutzer aus und können für jeden Benutzer unterschiedlich sein. GPOs und ihre Einstellungen gelten für Computer und Benutzer, mit denen sie verknüpft sind.

Group Policy Preferences (GPP) erweitern GPOs. Mit GPPs können Einstellungen für Computer und Benutzer vorgenommen werden, ohne den Benutzer an der Änderung der Konfiguration zu hindern. GPPs werden in SYSVOL in Form von XML-Dateien mit den entsprechenden Konfigurationseinstellungen erstellt. Manche GPPs bieten die Möglichkeit Zugangsdaten zu speichern und zu verwenden. Dazu gehören:

- Laufwerkszuordnungen (Drives.xml)
- Erstellung lokaler Benutzer
- Datenquellen (DataSources.xml)
- Druckerkonfiguration (Printers.xml)
- Dienste erstellen/aktualisieren (Services.xml)
- Scheduled Tasks (ScheduledTasks.xml)
- Änderung von Passwörtern lokaler Administratoren

In GPPs enthaltene Passwörter werden im Feld “cpassword” gespeichert und sind mit AES-256 Bit verschlüsselt. 2012 hat Microsoft jedoch den privaten AES-Schlüssel auf MSDN unbeabsichtigt veröffentlicht. Dieser kann zur Entschlüsselung von Passwörtern in GPPs verwendet werden. Da alle Domänenbenutzer Lesezugriff auf SYSVOL haben, kann jeder in der Domäne die SYSVOL-Freigabe nach XML-Dateien durchsuchen, die das Feld "cpassword" enthalten. Identifiziert ein Angreifer XML-Dateien, kann er den öffentlich bekannten AES-Key verwenden, um gespeicherte Passwörter zu entschlüsseln und sich gegebenenfalls Rechte in der Domäne auszuweiten.

Empfehlung

- Betrachtet gelistete Benutzerkonten als kompromittiert und ändert ihre Passwörter.
- Löscht vorhandene GPPs in SYSVOL, die Zugangsdaten enthalten. Microsoft hat ein PowerShell-Beispielskript für die Suche nach GPPs mit gespeicherten Passwörtern bereitgestellt (siehe Referenzen).
- Installiert KB2962486 auf allen Systemen, um zu verhindern, dass neue Zugangsdaten in Group Policy Preferences gespeichert werden.
- Die von Microsoft empfohlene Methode zum Ändern von Passwörtern lokaler Administratoren ist die "Local Administrator Password Solution" (LAPS).

Weiterführende Informationen

- https://support.microsoft.com/en-us/topic/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevation-of-privilege-may-13-2014-60734e15-af79-26ca-ea53-8cd617073c30

5. Zugangsdaten in Active Directory-Feldern

Remediation Status: Behoben
Kritikalität: High
CVSS-Score: 8.8
Empfehlung: Identifiziert vertrauliche Informationen in Feldern von Active Directory-Objekten und entfernt sie.

Überblick

Wir konnten im Zuge der Prüfung Passwörter von Benutzern identifizieren, die im Feld "Beschreibung" von Active Directory-Benutzerobjekten hinterlegt waren. Diese konnten erfolgreich für eine Anmeldung verwendet werden. Das Feld ist für alle authentifizierten Active Directory-Benutzer lesbar.

Anmerkungen zu Behebungsstatus

Während des Nachtests wurden keine Passwörter mehr im Feld "Beschreibung" von Active Directory-Benutzerobjekten gefunden.

Alle Passwörter wurden entfernt und geändert.

Beschreibung

Wir haben im Zuge der Prüfung festgestellt, dass bei folgenden Benutzern Zugangsdaten im Beschreibungsfeld gespeichert wurden.

- agathe.bauer@lab.local
- herbert.gurker@lab.local
- sqlsrv@lab.local

Jeder Domänenbenutzer kann standardmäßig viele Informationen von Objekten im Active Directory (AD) lesen, ohne über Administratorrechte verfügen zu müssen. Der Computer, von welchem auf die Informationen im AD zugegriffen wird, muss dazu nicht der Domäne angehören. Es genügt ein gültiges Domänenbenutzerkonto ohne spezielle Berechtigungen.

Das Feld "Beschreibung" ist dabei ein gängiger Speicherort für Administratoren, um sich selbst oder anderen Notizen zu bestimmten Konten zu machen. Diese Felder können auch von nicht privilegierten Benutzer gelesen werden.

Auch in anderen Feldern könnten unter Umständen vertrauliche Informationen gespeichert werden, beispielsweise in neuen Feldern bei Erweiterung des AD-Schemas.

Empfehlung

- Es sollte sichergestellt werden, dass keine vertraulichen Informationen in Feldern von Active Directory-Objekten gespeichert sind. Das Sysinternals-Tool "AD Explorer" bietet eine Suchfunktion, mit der jedes Feld für jedes Objekt in AD durchsucht werden kann.
- Die betroffenen Benutzerkonten sollten als kompromittiert betrachtet und ihre Passwörter geändert werden.
- Zum Austausch von Passwörtern und anderen sensiblen Daten sollten Passwortmanager verwendet werden.

6. Unconstrained Delegation für Dienstkonten

Kritikalität: High
CVSS-Score: 8.5
Betrifft: Dienstkonten IIS01-03
Empfehlung: Unconstrained Delegation sollte für Dienstkonten deaktiviert werden. Alternativ könnten Constrained Delegation oder Resource-based Constrained Delegation verwendet werden.

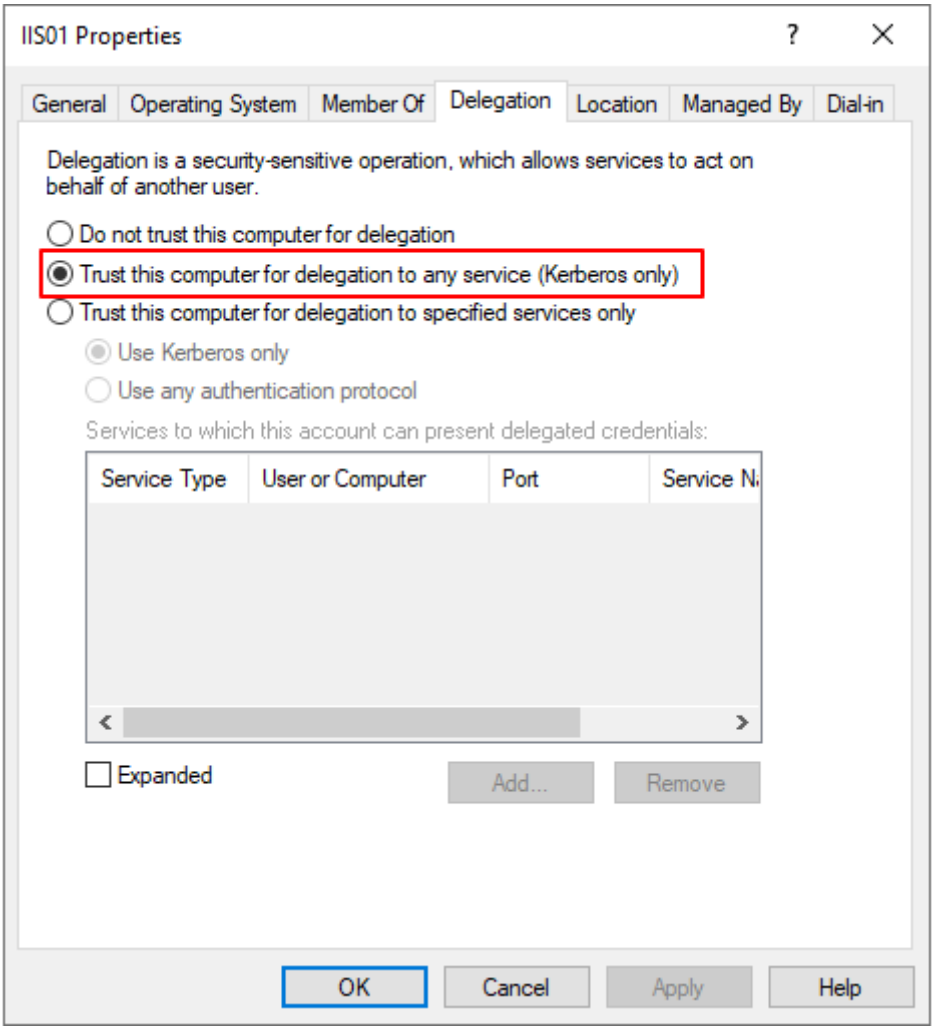
Überblick

Wir identifizierten drei Dienstkonten (IIS01-03) in der Active Directory-Domäne, für welche unsichere Kerberos Unconstrained Delegation konfiguriert waren. Angreifer, die eines dieser Dienstkonten erfolgreich kompromittieren, können auf zwischengespeicherte Authentifizierungstickets zugreifen. Auf den Domain Controllern ist zudem der Print Spooler Service aktiv. Dadurch kann ein Angreifer aktiv eine Authentifizierung der Domain Controller anstoßen, was diese Schwachstelle zusätzlich verschärft. Ein Angreifer könnte dadurch die Rechte eines Domänenadministrators erlangen.
Wir konnten die Schwachstelle nicht erfolgreich ausnutzen, da wir keines der drei Dienstkonten erfolgreich übernehmen konnten.

Beschreibung

Wir konnten im Zuge der Prüfung die folgenden Dienstkonten identifizieren, die für Unconstrained Delegation konfiguriert waren.

- IIS01
- IIS02
- IIS03



Konfiguration Unconstrained Delegation für IIS01

Wir konnten die Schwachstelle nicht erfolgreich ausnutzen, da wir keines der drei Dienstkonten erfolgreich übernehmen konnten. Es ist jedoch festzuhalten, dass die Administratoren der entsprechenden Webservices ihre Rechte auf jene eines Domänenadministrators erhöhen könnten.

Darüber hinaus identifizierten wir die folgenden Systeme mit aktiviertem Print Spooler Service:

- 10.17.1.10 - dc01.lab.local (Domain Controller)
- 10.17.1.20 - dc02.lab.local (Domain Controller)
- 10.17.1.30 - dc03.lab.local (Domain Controller)
- 10.17.1.34 - sql01.lab.local
- 10.17.1.40 - sql02.lab.local
- 10.17.1.44 - srv01.lab.local
- 10.17.1.139 - srv02.lab.local
- 10.17.1.172 - srv03.lab.local

Kerberos Delegation ermöglicht es Dienstkonten, sich gegenüber anderen Ressourcen im Netzwerk als andere Benutzer auszugeben (Impersonierung). Ein gängiges Beispiel ist ein Webserver, der einen Benutzer impersoniert, wenn er auf eine Backend-Datenbank zugreift und Daten im Sicherheitskontext dieses Benutzers abruft.

In Active Directory ist das Ticket Granting Ticket (TGT) die Berechtigung eines Benutzers, Ticket Granting Service (TGS)-Tickets für verschiedene Ressourcen der Domäne anzufordern. Verschlüsselte TGTs werden nach erfolgreicher Authentifizierung vom Domänencontroller ausgehändigt und können auch nur von diesem wieder entschlüsselt werden. Wenn ein Benutzer den Zugriff auf einen Dienst anfordert, validiert der Domänencontroller das TGT und erstellt daraufhin das gewünschte Service Ticket.

Wenn ein Benutzer ein Service Ticket für einen Dienst auf einem Server mit konfigurierter Unconstrained Delegation anfordert, wird eine Kopie des TGT in das TGS eingefügt. Der Server, dem das TGS letztendlich vorgelegt wird, kann das TGT des Benutzers extrahieren und zur späteren Wiederverwendung zwischenspeichern. Das bedeutet, der Server kann sich gegenüber jeder Ressource in der Domäne als dieser Benutzer ausgeben. Sobald ein Angreifer einen solchen Server kompromittiert, kann er das Service Ticket aus dem Speicher stehlen, das TGT extrahieren und sich als dieser Benutzer ausgeben und dessen Privilegien nutzen. Im schlimmsten Fall gelingt es einem Angreifer das TGT eines Domänenadministrators zu stehlen, wodurch er sich uneingeschränkt lateral im Netzwerk bewegen und die gesamte Domäne übernehmen könnte.

Die Ausnutzung von Unconstrained Delegation setzt voraus, dass Benutzer sich vorab mit dem Dienst verbinden. Ein Angreifer könnte dies beispielsweise mittels Phishing-Aktivitäten erreichen. Unter gewissen Voraussetzungen kann ein Angreifer eine Verbindung mit dem Dienst jedoch auch erzwingen. Eine Fehlfunktion im Windows Print System Remote Protocol, auch bekannt als Printer Bug, kann missbräuchlich verwendet werden, um Systeme mit aktiviertem Print Spooler Service andere Systeme nach Aktualisierungen von Druckaufträgen zu fragen. Das anfragende System erzwingt durch Aufruf der Funktion ein bestimmtes Zielsystem sich zu verbinden und sich mittels Service Ticket zu authentifizieren. Wenn das anfragende System für Unconstrained Delegation konfiguriert ist, würde das Service Ticket das TGT des Zielsystems enthalten. Standardmäßig läuft der Print Spool Service auf allen Windows Server Systemen. Ein Angreifer könnte damit sehr leicht an das TGT des Domänencontrollers kommen und die Domäne übernehmen.

Empfehlung

- Dienstkonten sollten nicht für Unconstrained Delegation konfiguriert sein. Wenn nötig, können stattdessen Constrained Delegation oder Resource-based Constrained Delegation verwendet werden.

- Privilegierte Benutzerkonten wie zum Beispiel Domänenadministratoren sollten der Sicherheitsgruppe "Protected Users" hinzugefügt werden. Mitglieder dieser Gruppe können nicht delegiert werden.
- Die Option "Account is sensitive and cannot be delegated" kann privilegierten Benutzerkonten gesetzt werden.
- Der Print Spooler Service sollte auf allen Systemen deaktiviert werden.

7. Benutzerkonten anfällig für Kerberoasting

Remediation Status: Teilweise Behoben
Kritikalität: High
CVSS-Score: 8.4
Betrifft: Service Accounts im Active Directory
Empfehlung: Die Passwörter der Dienstkonten sollten zufällig generiert und komplex sein, sowie mindestens 20 Zeichen lang sein. Die Berechtigungen der Dienstkonten sollten so weit wie möglich eingeschränkt werden.

Überblick

Wir identifizierten drei hoch privilegierte Dienstkonten (insgesamt: 4), die anfällig für Kerberoasting waren. Niedrig privilegierte Angreifer können Service-Tickets dieser Dienstkonten anfordern und das jeweilige Klartext-Passwort im Zuge eines Offline-Brute-Force-Angriff erraten. Bei Offline-Brute-Force-Angriffen können Passwörter erheblich schneller geknackt werden, als über das Netzwerk. Im Zuge der Prüfung konnten wir zwei Klartext-Passwörter erfolgreich knacken.

Anmerkungen zu Behebungsstatus

Im Zuge der Nachprüfung wurde festgestellt, dass die geknackten Passwörter von Service Accounts geändert wurden. Auskunftsgemäß entsprechen die neuen Passwörter den empfohlenen Komplexitätskriterien. Es wurde jedoch kein Mechanismus zur automatischen Änderung von Service Account Passwörtern implementiert, weshalb dieses Finding nur als teilweise behoben markiert wurde.

Beschreibung

Wir identifizierten im Zuge der Prüfung auf Kerberoasting anfällige Service Accounts. Hervorgehobene Konten waren Teil einer privilegierten Gruppe oder besaßen umfangreiche Berechtigungen. Die Übernahme eines dieser Konten hätte die vollständige Kompromittierung der gesamten Domäne zur Folge gehabt.

- **K5Admin**
- **SQLServer**
- **SRV**
- SSOUser

Alle Benutzer außer `SSOUser` waren direkt oder indirekt Teil der Domain-Administratoren Gruppe. Mittels eines Kerberoasting Angriffs war es möglich, das Passwort von mehreren Service Accounts zu erraten, wodurch die komplette Domäne

übernommen werden konnte. Im Zuge der Prüfungen wurden zwei der oben genannten Benutzer-Passwörter geknackt:

- K5Admin
- SQLServer

Beide Benutzer hatten schwache Passwörter konfiguriert (weniger als acht Zeichen).

Kerberoasting ist eine weit verbreitete Angriffstechnik, die Eigenschaften des Kerberos-Protokolls missbraucht. Kerberoasting ermöglicht es, gehashte Daten von Dienstkonten aus Service Tickets zu erlangen, um das Klartext-Passwort des jeweiligen Dienstes im Zuge eines Offline-Brute-Force-Angriff zu erraten.

Im Active Directory erlaubt das Ticket Granting Ticket (TGT) einem Benutzer, Ticket Granting Service (TGS)-Tickets für Ressourcen der Domäne anzufordern. Service Principle Names (SPNs) werden dabei zur eindeutigen Identifizierung jedes Dienstes innerhalb einer Windows-Domäne verwendet. Um die Authentifizierung zu ermöglichen erfordert Kerberos, dass SPNs mit einem Host- oder Domänenbenutzerkonto verknüpft werden. Angreifer mit gültigem TGT können ein oder mehrere TGS-Tickets für beliebige SPNs anfordern. Bei Verwendung des RC4-Algorithmus, sind Teile der TGS-Tickets mit dem NTLM-Hash des mit dem SPN verbundenen Dienstkontos verschlüsselt und somit anfällig für Offline-Brute-Force-Angriffe.

Kerberoasting funktioniert nur gegen SPNs von Domänenbenutzerkonten, da hostbasierte SPNs mit zufälligen 128-Zeichen langen Passwörtern gesichert sind, die alle 30 Tage automatisch geändert werden. Passwörter von Domänenbenutzerkonten laufen hingegen möglicherweise nie ab und werden in der Regel nur selten geändert. Häufig sind diese Passwörter schwach und leicht zu erraten.

Empfehlung

- Die RC4-Verschlüsselung für Tickets sollte durch eine AES-Verschlüsselung ersetzt werden.
- Die Passwörter der Dienstkonten sollten zufällig generiert und komplex sein, sowie mindestens 20 Zeichen lang sein.
- Den Einsatz von (Group) Managed Service Accounts könnte in Betracht gezogen werden. Diese speziellen Dienstkonten sind eine gute Methode, um sicherzustellen, dass die Passwörter lang und komplex sind, sowie regelmäßig geändert werden.
- Die Berechtigungen von Dienstkonten, sowie die Mitgliedschaft in privilegierten Gruppen wie z.B. Domänenadministratoren, sollte so weit wie möglich eingeschränkt werden.

8. Schwache Anforderungen an die Passwortkomplexität

Kritikalität: Medium
CVSS-Score: 5.9
Empfehlung: Es sollte eine strenge, dem Stand der Technik entsprechende Kennwortrichtlinie erzwungen werden.

Überblick

Zum Zeitpunkt der Prüfung waren schwache Kennwortrichtlinien in der Active Directory-Umgebung konfiguriert. Die erforderliche Passwortlänge betrug lediglich sieben Zeichen und es wurden keine Komplexitätsanforderungen erzwungen. Schwache Passwörter können in der Regel durch Brute-Force Angriffe in kurzer Zeit erraten werden. Bei erfolgreichem Erraten des Passworts eines privilegierten Benutzerkontos, könnte ein Angreifer die gesamte Domäne übernehmen.

Anmerkungen zu Behebungsstatus

Zum Zeitpunkt des Nachtests war die schwache Kennwortrichtlinie weiterhin aktiv.

Beschreibung

Die Kennwortrichtlinie zum Zeitpunkt der Prüfungen enthielt folgende Einstellungen, welche als unzureichend klassifiziert wurden:

- Mindestlänge von Passwörtern: 7 Zeichen
- Fehlende Komplexitätsanforderungen
- Passworthistorie: 3 Passwörter
- Mindestalter von Passwörtern: 1 Tag
- Maximalalter von Passwörtern: 180 Tage

Mechanismen zur Authentifizierung beruhen häufig auf einem gespeicherten Geheimnis (dem Passwort), um die Identität eines Benutzers zu bestätigen. Daher ist es sehr wichtig, dass Passwörter ausreichend sicher sind und von einem Angreifer nicht erraten werden können. Die konkreten Anforderungen an die Komplexität eines Passworts hängen von der Art der zu schützenden Umgebung und dem Benutzerkontext ab. Die Spezifikation geeigneter Passwortanforderungen und deren Durchsetzung sind entscheidend für eine sichere Authentifizierung. Ein schwaches Passwort wird durch ein oder mehrere Merkmale definiert. Es ist kurz (z. B kleiner als 8 Zeichen), wird häufig verwendet (Passwort123, Qwertz, ...), ist ein Standardpasswort (root, admin, guest, ...) oder kann schnell erraten werden (Sommer21, Winter2022, MaxMuster1, ...).

Schwache Passwörter ebnen daher den Weg für Angreifer, um diese mit automatisierten Methoden zu erraten. In der einfachsten Form könnte ein Angreifer

einen Brute-Force-Angriff durchführen. Dabei versucht ein Angreifer das Passwort eines Benutzerkontos zu erraten, indem er automatisiert zufällige Zeichenkombinationen durchprobiert. Oftmals werden bei einem solchen automatisierten Angriff auch sehr große Wortlisten verwendet, die häufig verwendete Passwörter oder Standardpasswörter beinhalten. So ein Angriff ist auch als Wörterbuchattacke bekannt. Sehr häufig testen Angreifer aber auch Zugangsdaten, die in Datenlecks veröffentlicht wurden. Diese spezielle Form des Brute-Force-Angriffs, wird als Credential Stuffing bezeichnet.

Gelingt es einem Angreifer Passwörter zu erraten, kann dieser betroffene Benutzerkonten übernehmen und im Kontext dieses Benutzers auf Funktionen und Daten in der Anwendung zugreifen. Bei Übernahme eines privilegierten Benutzerkontos, könnte ein Angreifer unter Umständen sogar die gesamte Domäne übernehmen.

Empfehlung

Die Anforderungen an Passwörter sollten mindestens folgenden Kriterien entsprechen:

- Mindestlänge von Passwörtern: 10 Zeichen
- Mindestlänge von Passwörtern für privilegierte Benutzer: 12 Zeichen
- Erzwungene Komplexitätsanforderungen
- Passworthistorie: 10 Passwörter
- Mindestalter von Passwörtern: 3 Tag

Als weiterführende Hilfestellung zur Definition einer modernen Kennwortrichtlinie, ist die NIST Richtlinie SP 800-63B in den Ressourcen verlinkt.

Weiterführende Informationen

- https://pages.nist.gov/800-63-3/sp800-63b.html

9. Netzwerkzugriff aufgrund fehlender NAC-Lösung

Remediation Status: Akzeptiert
Kritikalität: Medium
CVSS-Score: 4.3
Betrifft: Layer 2 Netzwerk/Netzwerkports am Standort Stephansplatz 1, 1010 Wien
Empfehlung: Stellt sicher, dass Geräte für den Zugang in Ihr Unternehmensnetzwerk auf Basis des 802.1X Standards authentifiziert und autorisiert werden.

Überblick

Wir konnten uns im Zuge der Prüfung Zugang zum Unternehmensnetzwerk aufgrund einer fehlenden Network Access Control (NAC)-Lösung verschaffen. NAC ist eine Maßnahme, die sicherstellt, dass nur vertrauenswürdige Geräte eine Verbindung zum Unternehmensnetzwerk herstellen dürfen und dass diese alle Anforderungen des Netzwerks erfüllen, bevor sie Zugang erhalten. Nicht vertrauenswürdige und nicht autorisierte Geräte werden dadurch vom Netzwerk ferngehalten. Wenn jedoch keine NAC-Lösung im Unternehmen etabliert ist, können Angreifer Computer, Computerzubehör oder Netzwerkhardware im Netzwerk platzieren, die als Ausgangspunkt für den Zugriff auf interne Ressourcen genutzt werden können.

Anmerkungen zu Behebungsstatus

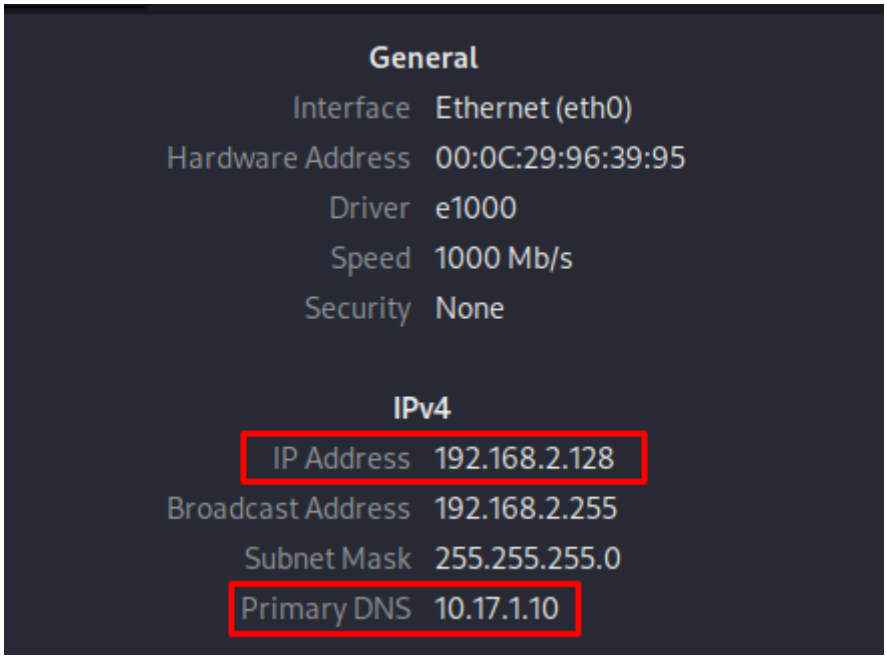
Der Auftraggeber akzeptiert das Risiko von Netzwerkzugriff durch unautorisierte Geräte. Es ist nicht geplant in Zukunft 802.1X zu implementieren.

Beschreibung

Wir konnten uns initialen Zugang zum Unternehmensnetzwerk verschaffen, indem wir unsere Arbeitsgeräte direkt an die vor Ort vorgefundenen freien LAN-Buchsen angeschlossen haben. Da es keine Einschränkungen hinsichtlich Netzwerkzugang gab, konnten wir auf interne Ressourcen und das Internet zugreifen.

Firmenfremder Switch an Netzerkbuchse

Folgende Abbildung zeigt, dass das firmenfremde Gerät via DHCP eine IP sowie DNS Server und Gateway zugewiesen bekam. Es war weiters möglich, am selben LAN-Port (über einen Netzwerk-Switch) mehrere Geräte an derselben LAN-Dose anzuhängen.



Automatische Zuweisung einer IP-Adresse via DHCP an firmenfremdes Gerät

Wir konnten somit auf interne Ressourcen und das Internet zugreifen.

Network Access Control (NAC) ermöglicht es Richtlinien für den Zugang in ein Unternehmensnetzwerk zu definieren und durchzusetzen. Wenn ein Computer beispielsweise eine Verbindung zu einem Netzwerk herstellt, darf er nur dann auf Ressourcen zugreifen, wenn er die vom Unternehmen festgelegte Richtlinie erfüllt (z. B. Virenschutz, aktuelle Systemversion, bestimmte Konfiguration, etc.). Sobald die Richtlinie erfüllt ist, kann der Computer im Rahmen der von der NAC-Lösung festgelegten Richtlinie auf Netzwerkressourcen und das Internet zugreifen. Die grundlegende Form von NAC ist der 802.1X-Standard.

802.1X ist ein Authentifizierungsstandard für Geräte, die sich mit einem geschützten LAN oder WLAN verbinden möchten. Nur authentifizierte und autorisierte Geräte erhalten Zugang zu geschützten Netzwerken. Bei einer 802.1X-Authentifizierung sind drei Komponenten beteiligt: ein Supplicant, ein Authenticator und ein Authentication Server. Der Supplicant ist ein Gerät (z. B. ein Laptop), das sich mit dem LAN / WLAN verbinden möchte. Der Authenticator ist ein Netzwerkgerät (z. B. ein Switch oder Access-Point), das die Verbindung zwischen dem Client und dem Netzwerk herstellt. Der Authentication Server ist ein Server, der Supplicants (d. h. Client-Geräte) authentifiziert und darüber entscheidet, ob der Zugang eines Supplicants in ein geschütztes Netzwerk zugelassen werden soll. Der Authentication Server ist dazu an einen Identity Store (wie z. B. LDAP) angebunden.

Für die Authentifizierung wird das Extensible Authentication Protocol (EAP) verwendet, das eine sichere Methode zur Übermittlung von Anmeldeinformationen für die Netzwerkauthentifizierung bietet. 802.1X ist der Standard, der für die Übertragung von EAP-Nachrichten über drahtgebundene oder drahtlose Netzwerke verwendet wird. Über

einen verschlüsselten EAP-Tunnel verhindert 802.1X, dass Informationen von Dritten mitgelesen werden können. Das EAP-Protokoll bietet verschiedene Möglichkeiten der Authentifizierung wie z. B. über Benutzername/Passwort (EAP-TTLS/PAP und PEAP-MSCHAPv2) oder über Client-Zertifikate (EAP-TLS) an.

Empfehlung

- Implementiert eine NAC-Lösung auf Basis von 802.1X zur sicheren Authentifizierung und Autorisierung von Geräten in Ihrem Netzwerk.
- Verwendet EAP-TLS, um Geräte per Zertifikate zu authentifizieren.
- Erzwingt MAC Authentication Bypass (MAB) für Geräte, die 802.1X nicht unterstützen. Stellt sicher, dass diese Geräte durch entsprechende Netzwerksegmentierung abgeschottet werden.
- Blockiert generell den Netzwerkzugang für unbekannte Geräte.
- Asset-Management-Lösungen können bei der Erkennung von unbekannten Geräten im Netzwerk helfen.

10. Windows Active Directory Audit

0.0
Betrifft: Active Directory-Benutzerobjekte
Empfehlung: Der Gesundheitszustand der Domäne sollte regelmäßig überwacht werden, um Sicherheitsrisiken zu minimieren

Überblick

Im Rahmen des Penetration-Tests wurden die in Active Directory gespeicherten User- und Computer-Objekte analysiert und verschiedene Metriken ausgewertet.

Beschreibung

Im Rahmen des Penetration-Tests wurden Active Directory-Objekte analysiert und Metriken ausgewertet. Dadurch wurde die aktuelle Situation innerhalb der Active Directory Domain bewertet.

Benutzer-Statistiken

Beschreibung	Anzahl	Prozent
Aktive Benutzer	1102	97%
Inaktive Benutzer	32	3%
Passwort vor mehr als 1 Jahr geändert	402	35%
Passwort vor mehr als 5 Jahren geändert	281	24%
Kennwort läuft nie ab	103	9%
Aktive Benutzer die sich nie angemeldet haben	97	9%
Benutzer-Delegation erlaubt	1097	96%
Kennwort nicht erforderlich	0	0%
Kennwörter mit umkehrbarer Verschlüsselung gespeichert	0	0%
Benutzer mit deaktivierter Kerberos Pre-Authentication	0	0%

In der Active Directory Domain existieren viele aktive Benutzer, die nicht mehr verwendet werden. Diese sollten deaktiviert werden. Des Weiteren war die Delegation von fast allen Benutzerkonten - inklusive hoch priviligierten Benutzer - erlaubt. Dies sollte zumindest für hoch privilegierte Benutzer deaktiviert werden. Knapp 700 Benutzer haben ihr Passwort seit mehr als einem Jahr nicht mehr geändert. Es könnte angedacht werden,

nach dem Anpassen der Kennwortrichtlinien, die Passwörter aller Benutzer zurückzusetzen, um komplexe Passwörter zu erzwingen.

Priviligierte Gruppen-Statistiken

Gruppenname	Anzahl Gruppenmitgleider
ADMINISTRATORS@LAB.LOCAL	27
DOMÄNEN-ADMINS@LAB.LOCAL	16
ORGANISATIONS-ADMINS@LAB.LOCAL	4
SCHEMA-ADMINS@LAB.LOCAL	4
SERVER OPERATORS@LAB.LOCAL	12
ACCOUNT OPERATORS@LAB.LOCAL	6
BACKUP OPERATORS@LAB.LOCAL	16
PRINT OPERATORS@LAB.LOCAL	33
CERT PUBLISHERS@LAB.LOCAL	15
DNS ADMINS@LAB.LOCAL	1

27 Benutzer waren zum Zeitpunkt der Prüfung in der Gruppe "Administrators". Durch diese Berechtigung sind die Benutzer auch lokale Administratoren auf den Domain Controllern. Dort könnten sich diese Benutzer zur Gruppe der Domänenadministratoren hinzufügen und ihre Rechte erweitern. Diese Benutzer sind daher als gleichwertig zu Domänenadministratoren zu betrachten und sollten auf ein Minimum reduziert werden. Zum Zeitpunkt der Prüfung gab es 16 Domänenadministratoren. Dies ist angesichts der Größe der Infrastruktur als hoch einzuschätzen. Die Zahl der Domänenadministratoren sollte so weit wie möglich gesenkt werden.

Computer-Statistiken

Zum Zeitpunkt der Prüfung waren 871 Maschinenkonten in der Active Directory Domain registriert. Folgende Tabelle zeigt die verwendeten Betriebssysteme und deren Versionen.

Betriebssystem	Anzahl
Microsoft Windows Server 2003 Service Pack 2	1
Windows XP for Embedded Systems	5
Microsoft Windows Server 2008 R2 Standard Service Pack 1	3
Microsoft Windows Server 2008 R2 Foundation Service Pack 1	1
Microsoft Windows Server 2016 Standard	7

Betriebssystem	Anzahl
Microsoft Windows 7 Professional	23
Microsoft Windows 10 Pro	831

17 Computer und Server verwendeten zum Zeitpunkt der Prüfung nicht mehr unterstützte Betriebssysteme.

Empfehlung

- Die Anzahl der Domain Administratoren und anderer hoch privilegierter Konten sollte auf ein Minimum beschränkt werden
- Benutzer, die sich längere Zeit nicht angemeldet haben, sollten auf "inaktiv" gesetzt werden.
- Nach der Implementierung einer strengeren Kennwortrichtlinie, empfehlen wir die Passwörter aller Benutzer einmalig zurückzusetzen.
- Computer mit nicht unterstützten Betriebssystem-Versionen sollten deprovisioniert oder aktualisiert werden.

Änderungsverzeichnis

Version	Datum	Beschreibung	Autor
0.1	2022-09-09	Initiale Erstellung	Aron Molnar
1.0	2022-09-12	Review und Freigabe	Patrick Pirker

Disclaimer

Wir können nicht garantieren, dass alle vorhandenen Schwachstellen und Sicherheitsrisiken tatsächlich entdeckt wurden. Das ist den beschränkten Zeitressourcen und dem limitierten Wissen der Pentester über die IT-Infrastruktur, Software, Source-Code, Benutzer etc. geschuldet. Eine umfassende Zusammenarbeit zwischen Auftraggeber und Penetration Testern erhöht die Effizienz des Penetration Tests. Das umfasst zum Beispiel die Offenlegung von Details interner Systeme oder die Provisionierung von Test-Benutzern.

Dieser Penetration Test stellt eine Momentaufnahme zum Zeitpunkt der Prüfung dar. Es lassen sich keine zukünftigen Sicherheitsrisiken davon ableiten.

Impressum

syslifters.com | **Dedicated to Pentests.**
Syslifters GmbH | Eitzersthal 75 | 2013 Göllersdorf
FN 578505 v | Bezirksgericht Hollabrunn