الجمهورية العربية السورية

وزارة التعليم العالي والبحث العلمي

جامعة تشرين – كلية الهندسة المعلوماتية

قسم النظم والشبكات الحاسوبية

دراسة مرجعية حول

Active Direcotry Attacks

(golden ticket and SyncDC attack)

إعداد الطلاب:

حيدر أيمن زينو

حلا غياث عمران

حسين محمد سعيد شنن

إشراف:

د. روني قسام

العام الدراسي 2024-2025

ان هذه المعلومات تم اخذها من ::

باسم إبراهيم مختار1، وأنكا د. جوركوت 2، ومحمود سعيد السيد 2،* وماريان أ. عازر 1،3

1 كلية تكنولوجيا المعلومات وعلوم الكمبيوتر، جامعة النيل، القاهرة 12566، مصر

2 كلية علوم الكمبيوتر، كلية دبلن الجامعية، D04V1W8 دبلن، أيرلندا

3 قسم الحاسبات والأنظمة، المعهد القومي للاتصالات، القاهرة 12577، مصر

*** المراسلة: mahmoud.abdallah@ucdconnect.ie**

1- ما هو ال DC

هو إطار عمل من شركة مايكروسوفت يُستخدم لإدارة الموارد والشبكات في بيئات المؤسسات. تم تطويره خصيصًا لأنظمة التشغيل **Windows Server**، ويوفر نظامًا مركزيًا لإدارة المستخدمين، الأجهزة، والتطبيقات، بالإضافة إلى تأمين الوصول إلى الشبكة. يُعتبر أحد المكونات الأساسية لأي شبكة كبيرة.

1.1 - المكونات الرئيسية :

Active Directory (AD): هو نظام من مايكروسوفت يُستخدم لإدارة الموارد والشبكات في المؤسسات، ويعمل على تنظيم المستخدمين، الأجهزة، والتطبيقات بشكل مركزي. يُعد النطاق (Domain) العنصر الأساسي فيه، حيث يتم التحكم بجميع الموارد من خلال خادم مركزي يُسمى Domain Controller (DC). يتيح Active Directory إدارة الوحدات التنظيمية (Organizational Units) لتطبيق السياسات الجماعية (Group Policies) التي تتحكم في

إعدادات الأجهزة والمستخدمين. يوفر النظام اتصالًا بين نطاقات متعددة داخل هيكل شجرة (Tree) أو غاب (Forest)، مما يتيح للمؤسسات إدارة الشبكات الكبيرة بكفاءة. يعتمد على بروتوكول المصادقة Kerberos لتأمين عمليات تسجيل الدخول، ويُمكن من خلاله تطبيق سياسات أمان جيدة، إدارة الحسابات، والتحكم في الأجهزة المتصلة AD . يُعتبر أداة أساسية للشركات التي تسعى إلى تنظيم مواردها وتأمين شبكاتها بطريقة مرنة ومركزية.

1.2 - أهمية دراسة الهجمات على DC:

- **كشف نقاط الضعف:**

دراسة الهجمات تساعد على تحديد الثغرات الشائعة مثل سوء إعداد الصلاحيات، كلمات المرور الضعيفة، أو الثغرات في بروتوكولات المصادقة مثل Kerberos.

- **تعزيز الأمن السيبراني:**

فهم كيفية استغلال المهاجمين لـ AD يمكن فرق الأمن من تطبيق سياسات وإعدادات تمنع تلك الهجمات، مثل تقوية إعدادات Group Policy، وتفعيل تسجيل الأنشطة (Auditing).

- **الاستعداد للهجمات المتقدمة:**

العديد من الهجمات المتطورة مثل **Kerberoasting** و**Pass-the-Hash** تستهدف AD . دراسة هذه التقنيات تساعد على تصميم دفاعات استباقية.

- **ضمان استمرارية الأعمال:**

الهجمات على AD قد تؤدي إلى تعطيل الوصول إلى البيانات والخدمات الحيوية. دراسة الهجمات تمنح المؤسسات أدوات لمنع التوقف عن العمل أو تقليل تأثيره.

- **الالتزام بالقوانين والمعايير:**

فهم الهجمات يساعد في الالتزام بمعايير الأمان المطلوبة مثل ISO 27001 وGDPR، التي تتطلب حماية البيانات والتحكم في الوصول.

- **التدريب العملي للفرق الأمنية:**

دراسة الهجمات تُثري معرفة فرق الأمن وتعطيهم فهمًا عمليًا لكيفية الكشف عن الهجمات في مراحلها الأولى ومعالجتها.

- **تقليل التكلفة الناتجة عن الاختراقات:**

الهجمات الناجحة على AD تؤدي إلى خسائر مالية كبيرة بسبب الفدية أو استعادة الأنظمة. الوقاية من خلال الفهم المتعمق لهذه الهجمات يمكن أن يقلل تلك التكاليف.

- **مواكبة التهديدات الجديدة:**

تقنيات الهجوم على AD تتطور باستمرار. دراسة الهجمات الحديثة تساعد في تطوير استراتيجيات جديدة للحماية.

- **تأمين بيانات المستخدمين والمؤسسة:**

AD يحتوي على بيانات حساسة عن المستخدمين، الأجهزة، وأدوارهم. حماية هذه البيانات من التسريب أو التلاعب هي أولوية قصوى.

Golden Ticket Attack – 2

ماهو Kerberos؟

هو بروتوكول مصادقة آمن تم تطويره لتوفير آلية موثوقة لإثبات هوية المستخدمين والخوادم على شبكة غير آمنة. وقد سُمي على اسم "**كلب كيربيروس** "، الكلب الأسطوري ثلاثي الرؤوس الذي كان يحرس مدخل العالم السفلي في الميثولوجيا الإغريقية. تمامًا كما كان Kerberos يحرس المدخل، فإن البروتوكول يضمن عدم وصول أي شخص غير مصرح له إلى الموارد.

آلية عمل بروتوكول Kerberos:

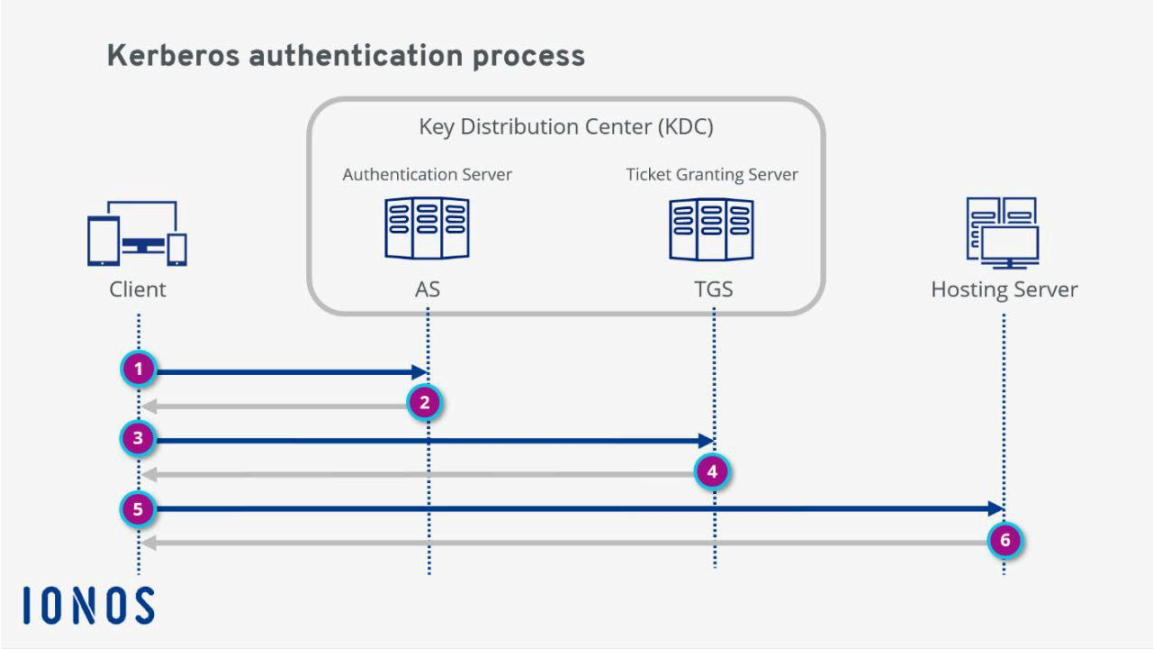
تشبه آلية المصادقة في كيربيروس عمل الكلب ثلاثي الرؤوس، حيث يلعب كل رأس دورًا في حراسة عملية المصادقة. العملية تشمل ثلاث مراحل رئيسية بمشاركة ثلاثة عناصر رئيسية:

رأس أول: العميل– (Client) : هذا هو الكيان الذي يسعى للوصول إلى خدمة معينة على الشبكة، ويبدأ العملية من خلال إرسال طلب مصادقة إلى الخادم.

رأس ثاني: خادم المصادقة– (AS) : هذا الخادم يتحقق من هوية العميل باستخدام بيانات المصادقة (مثل كلمة المرور) ويصدر تذكرة مؤقتة تسمى **TGT** (Ticket Granting Ticket) إذا تم التحقق بنجاح

رأس ثالث: خادم منح التذاكر– (TGS) : بعد أن يحصل العميل على الـ **TGT** من خادم المصادقة، يرسلها إلى خادم منح التذاكر للحصول على تذكرة خدمة (Service Ticket) للوصول إلى خدمة معينة على الشبكة.

هذه المراحل تتكامل معًا لضمان عملية مصادقة آمنة ودون الحاجة لإرسال كلمات المرور عبر الشبكة، مما يعزز من الأمان ويقلل من مخاطر السرقة أو التنصت على البيانات وهذا الشكل يوضح اليه عمل البروتكول.



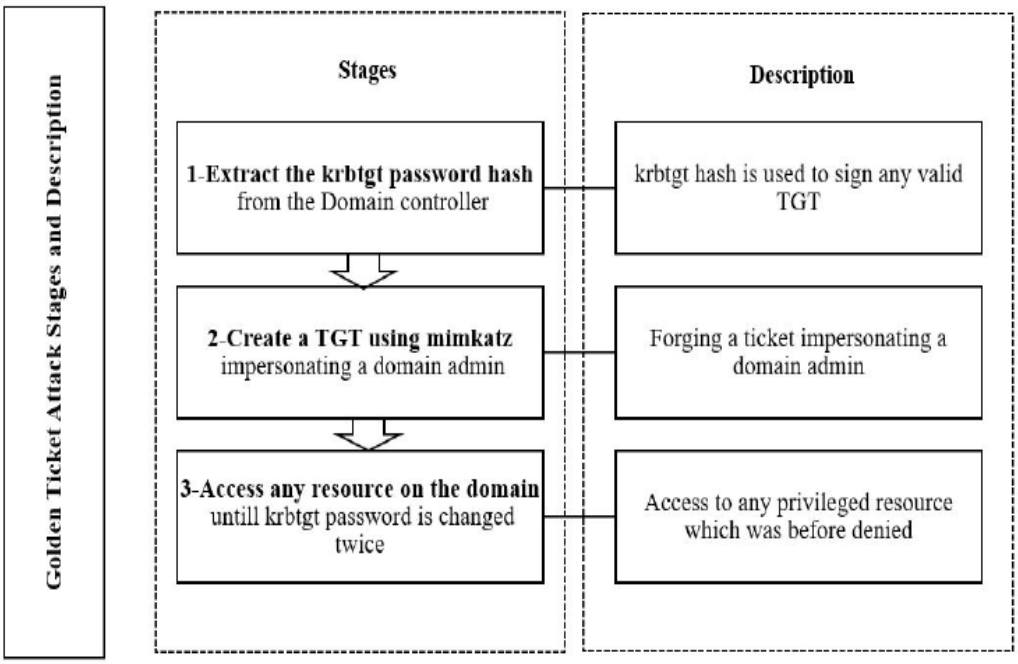
ما هي التذاكر في Kerberos:

تذكرة منح التذاكر ticket granting ticket:

في Kerberos، يُعتبر **TGT (Ticket Granting Ticket)** مكونًا رئيسيًا في عملية المصادقة، حيث يُستخدم للسماح للمستخدم بالوصول إلى الخدمات دون الحاجة لإعادة إدخال كلمة المرور بشكل

متكرر. يتم إصدار TGT بواسطة **Key Distribution Center (KDC)** بعد أن يتحقق من هوية المستخدم عند تسجيل الدخول الأولي. يتم تشفير TGT بمفتاح سري خاص بخدمة **Ticket Granting Service (TGS)**، مما يجعله غير قابل للتعديل أو التزوير. عندما يسجل المستخدم الدخول، يقوم بإرسال اسم المستخدم إلى KDC، وإذا تم التحقق بنجاح، يُصدر KDC الـ TGT ويعيده إلى العميل مع مفتاح جلسة مشترك. يُخزن TGT مؤقتًا على جهاز المستخدم ويظل صالحًا لفترة محدودة (عدة ساعات عادةً). لاحقًا، عندما يريد المستخدم الوصول إلى خدمة معينة، يرسل TGT الخاص به إلى TGS لطلب **تذكرة خدمة (Service Ticket)**، وعند التحقق من صلاحية TGT، يصدر TGS تذكرة الخدمة التي يتم استخدامها للوصول إلى الخادم المستهدف.

يتميز TGT بالأمان بفضل التشفير وصلاحيته المؤقتة، مما يقلل من احتمالية إساءة استخدامه. يعمل TGT كجزء من نظام **Single Sign-On (SSO)** في Kerberos، مما يجعل العملية أكثر كفاءة حيث يتيح للمستخدم المصادقة مرة واحدة لكل جلسة عمل، وبدون الحاجة لإرسال كلمة المرور بشكل متكرر عبر الشبكة.



تذكرة منح الخدمة Ticket Granting Service:

في Kerberos، **تذكرة منح الخدمة (Ticket Granting Service – TGS)** هي المرحلة الثانية في عملية المصادقة بعد الحصول على **تذكرة منح التذاكر (TGT)**، حيث تُستخدم لتوفير تذاكر خدمة تتيح للمستخدم الوصول إلى موارد أو خدمات محددة داخل النظام. عندما يريد المستخدم الوصول إلى خدمة معينة، مثل خادم ملفات أو قاعدة بيانات، يقوم بإرسال طلب إلى خادم TGS، ويتضمن الطلب **TGT** الذي حصل عليه سابقًا من خادم المصادقة (AS)، بالإضافة إلى اسم الخدمة التي يريد الوصول إليها. يقوم TGS بالتحقق من صلاحية TGT، ويستخدم المفتاح السري الخاص به لفك تشفيره للتأكد من أنه لم يتم تعديله أو تزويره. إذا كان TGT صالحًا، يُصدر TGS **تذكرة خدمة**

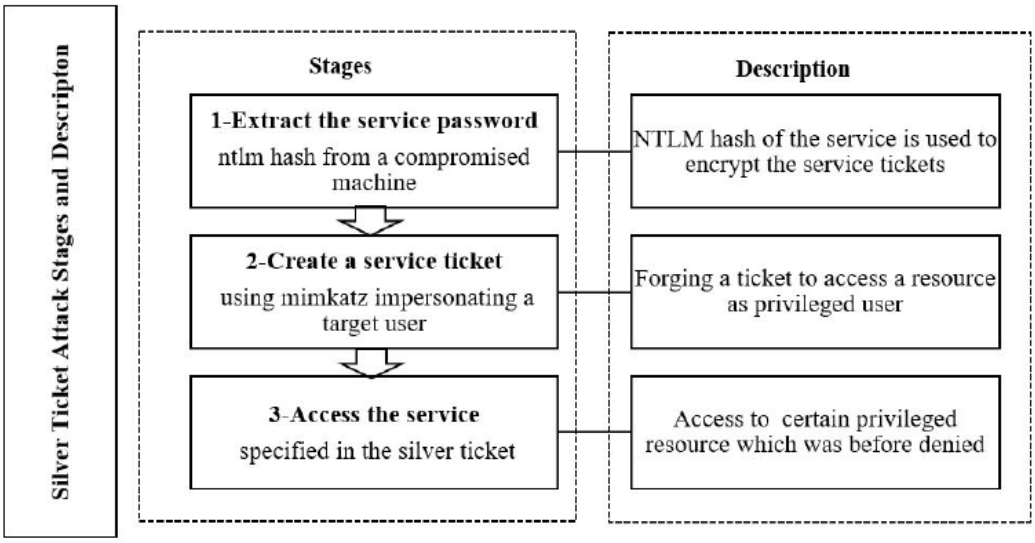
(Service Ticket) مشفرة باستخدام المفتاح السري الخاص بالخدمة المطلوبة، إلى جانب مفتاح جلسة مشترك بين العميل والخدمة. تُعاد تذكرة الخدمة إلى العميل، الذي يقوم بدوره بإرسالها إلى الخدمة المستهدفة للوصول إليها. إذا تحققت الخدمة من صلاحية التذكرة وكانت صحيحة، يتم منح المستخدم الإذن للوصول. تتميز تذكرة منح الخدمة بأنها تمنح المستخدم الوصول الآمن والمرن إلى الموارد دون الحاجة إلى إعادة المصادقة مع KDC في كل مرة، وتعمل جنبًا إلى جنب مع TGT لضمان عملية **Single Sign-On (SSO)**، حيث يكتفي المستخدم بالمصادقة مرة واحدة خلال الجلسة.

يتم تشفير التذاكر والمفاتيح باستخدام مفاتيح سرية لضمان أمان العملية، وتكون تذاكر الخدمة صالحة لفترة زمنية محددة لمنع أي استخدام غير مصرح به بعد انتهاء صلاحيتها.

تذكرة منح الخدمة Ticket Service:

في Kerberos، **تذكرة الخدمة (Service Ticket – ST)** هي المرحلة الأخيرة في عملية المصادقة، حيث تُستخدم للوصول إلى الخدمة المستهدفة بشكل آمن بعد الحصول عليها من **TGS (Ticket Granting Service)**. عندما يريد المستخدم الوصول إلى خدمة معينة (مثل خادم ويب أو قاعدة بيانات)، يرسل طلبًا إلى TGS يحتوي على **TGT (Ticket Granting Ticket)** واسمه واسم الخدمة المطلوبة. يقوم TGS بالتحقق من صلاحية TGT، وإذا كان صالحًا، يصدر **تذكرة الخدمة (ST)**. يتم تشفير تذكرة الخدمة باستخدام مفتاح سري خاص بالخدمة المستهدفة، ما يعني أن الخدمة فقط يمكنها فك تشفيرها والتحقق من صحتها. تحتوي ST على معلومات مثل هوية المستخدم، عنوان IP، وقت انتهاء الصلاحية، ومفتاح جلسة مشترك بين العميل والخدمة، مما يتيح

لهما التواصل بشكل آمن. بمجرد أن يتلقى العميل ST، يرسلها إلى الخدمة المستهدفة كجزء من طلبه. تتحقق الخدمة من التذكرة عن طريق فك تشفيرها باستخدام مفتاحها الخاص، وإذا كانت صالحة، يُمنح المستخدم الإذن للوصول إلى الموارد المطلوبة. تتميز ST بأنها تُستخدم مرة واحدة لكل خدمة، ما يعزز الأمان ويقلل من خطر إساءة استخدامها. كما أنها جزء من نظام **Single Sign-On (SSO)**، حيث يتيح Kerberos للمستخدم الوصول إلى عدة خدمات خلال الجلسة نفسها دون الحاجة لإعادة إدخال كلمة المرور. يعمل تصميم ST على ضمان سرية البيانات وسلامتها أثناء الاتصال بين المستخدم والخدمة، ويظل استخدامها مقيدًا بفترة زمنية محددة لتقليل مخاطر الاختراق أو التزوير.

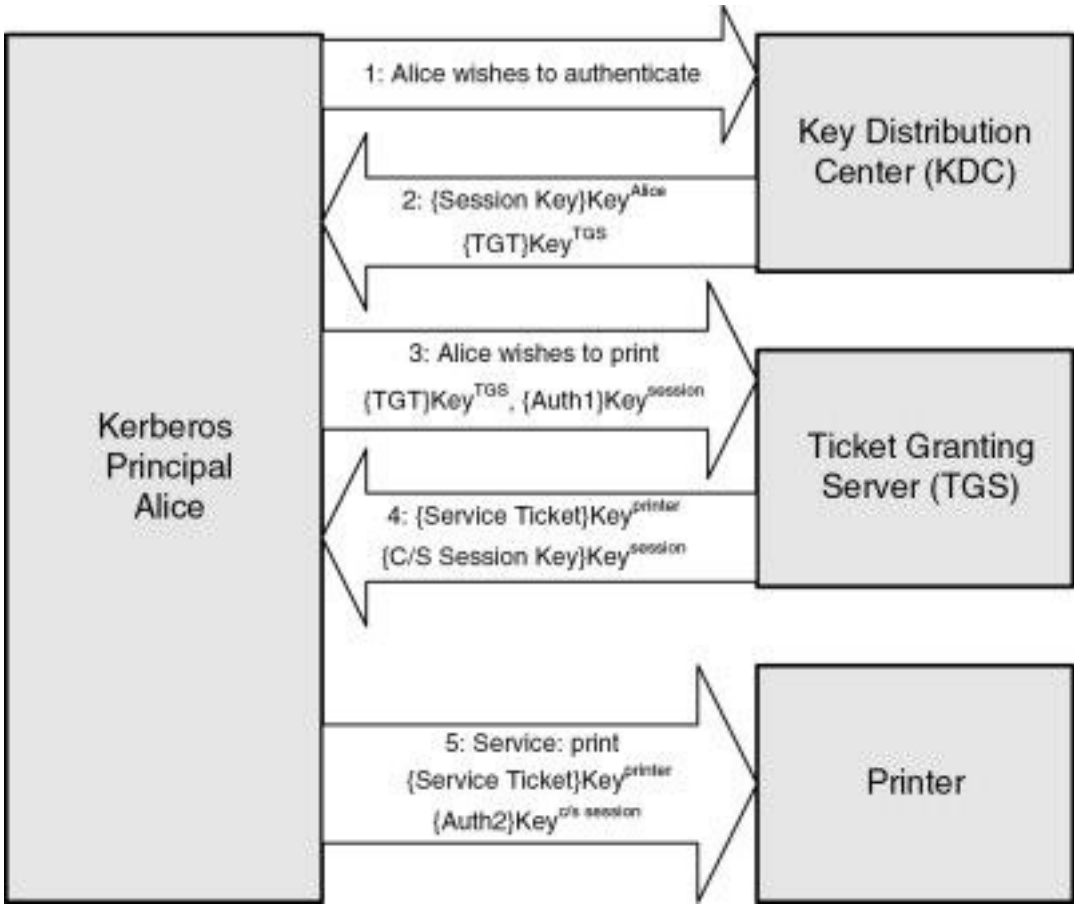


- **الهجوم على TGT (Ticket Granting Ticket)**: إذا تمكن المهاجم من الحصول على كلمة مرور أحد المستخدمين (سواء عن طريق التصيد الاحتيالي، أو القوة الغاشمة، أو تسريب كلمات المرور)، يمكنه استخدامها لتوليد TGT صالح. من خلال هذا الـTGT ، يستطيع المهاجم طلب تذاكر

TGSلخدمات متعددة دون الحاجة إلى المصادقة مجددًا، مما يمنحه وصولاً غير محدود تقريبًا خلال فترة صلاحية التذكرة.

•**الهجوم على :(TGS (Ticket Granting Service** في حال تمكن المهاجم من اعتراض أو سرقة TGT أثناء التنقل (مثلًا عبر هجمات الوسيط MITM)، قد يتمكن من التلاعب به أو إعادة استخدامه لطلب تذاكر TGS صالحة لخدمات معينة داخل الشبكة، مما يمنحه وصولًا إلى موارد لا يُفترض أن يكون لديه إذن للوصول إليها.

•**الهجوم على ST (Service Ticket)**: إذا نجح المهاجم في الحصول على Service Ticket، إما عن طريق السرقة أو الاستحواذ على الجلسة، فسيتمكن من الوصول إلى الخدمة المرتبطة بالتذكرة دون الحاجة إلى إعادة المصادقة. تعتبر هذه التذاكر صالحة لفترة محددة، مما يعني أن المهاجم يمكنه استغلالها خلال تلك الفترة للوصول إلى الخدمة.



الفكرة الأساسية للهجوم :

في البداية، يعتمد Kerberos على مبدأ التذاكر (Tickets) لتوثيق دخول المستخدمين إلى الشبكة. عندما يحتاج المستخدم إلى الوصول إلى خدمة معينة على الشبكة، يحصل على TGT من خادم المصادقة (AS)، ثم يستخدم هذا الـ TGT للحصول على تذاكر خدمة **من** خادم منح التذاكر (TGS). بشكل طبيعي، يُصدر TGT من KDC (Key Distribution Center) الذي يحتوي على مفتاح مخصص يسمى KRBTGT، وهو مفتاح سرّي يُستخدم لتشفير جميع التذاكر.

كيف يتم الهجوم؟

الوصول إلى حساب الKRBTGT:

لكي يتمكن المهاجم من تنفيذ هجوم Golden Ticket، يجب عليه أولاً أن يحصل على حقوق الوصول إلى حساب KRBTGT. يمكن تحقيق ذلك من خلال اختراق حساب مسؤول (Domain Admin) في الشبكة. بمجرد أن يحصل المهاجم على هذه الصلاحيات، يتمكن من الحصول على مفتاح KRBTGT، وهو سرّي ويمثل القلب في عملية المصادقة باستخدام Kerberos.

إنشاء التذكرة المزورة:

بعد الحصول على مفتاح KRBTGT، يقوم المهاجم باستخدامه لإنشاء تذاكر مزورة من نوع Golden Ticket. هذه التذاكر تكون تذاكر TGT مزورة، وهي مُشفرة بنفس الطريقة التي يُشفر بها التذكرة الأصلية الصادرة عن خادم المصادقة. كما أن هذه التذاكر تحتوي على معلومات يمكن تعديلها مثل اسم المستخدم، صلاحيات الحساب، الوقت المحدد للصلاحية، والعديد من التفاصيل الأخرى.

الانتشار عبر الشبكة:

عندما يقوم المهاجم باستخدام الـ **Golden Ticket**، فإنه يحصل على تذكرة **TGT** صالحة يمكن استخدامها للوصول إلى أي خدمة داخل الشبكة، بما في ذلك الأنظمة ذات الصلاحيات العالية مثل الخوادم أو قواعد البيانات. بما أن هذه التذاكر تبدو كأنها صادرة من **KDC** الشرعي، فإنه من الصعب اكتشاف أنها مزورة. الهجوم يتيح للمهاجم الوصول إلى جميع الموارد بدون أن يضطر إلى استخدام كلمة المرور الحقيقية للحسابات.

التغطية على الهجوم:

المهاجم يمكنه تحديد **صلاحية التذكرة** إلى مدة طويلة جداً (قد تصل إلى عدة سنوات)، مما يعني أنه حتى بعد تنفيذ الهجوم، قد تكون التذاكر صالحة لفترات زمنية طويلة. من الصعب جدًا اكتشاف الهجوم

لأن التذاكر المزورة لا تظهر كأنها مشبوهة، بل هي جزء من البروتوكول الطبيعي. كما أن المهاجم يمكنه تغيير توقيت التذكرة بما يتناسب مع حاجة الهجوم.

التداعيات الخطيرة للهجوم

الوصول غير المحدود: يمكن للمهاجم الوصول إلى جميع الموارد على الشبكة، بما في ذلك الأجهزة والبيانات الحساسة، مما يشكل تهديدًا أمنيًا خطيرًا.

استمرار الهجوم: يمكن لـ Golden Ticket أن يبقى صالحًا لفترة طويلة (حتى عدة سنوات)، مما يتيح للمهاجم إمكانية العودة إلى الشبكة واستخدام التذاكر في أي وقت.

التحكم الكامل في الشبكة: بمجرد أن يسيطر المهاجم على الـ **Golden Ticket**، فإنه يمكنه تنفيذ أي عملية على الشبكة، بما في ذلك تثبيت البرمجيات الخبيثة، سرقة البيانات، أو تعطيل الخدمات.

نشأ مفهوم **Golden Ticket** من باحث ومطور أمني يُدعى **بنيامين ديلبي**، والمعروف بإنشاء أداة قوية لُقبت بما بعد الاستغلال تُدعى "Mimikatz" ، وهي أداة لإلقاء بيانات الاعتماد قادرة على الحصول على بيانات تسجيل الدخول وكلمات المرور لحسابات Windows بصيغة نصية عادية. يستغل هجوم التذكرة الذهبية Kerberos، خدمة المصادقة الافتراضية لـActive Directory ، عن طريق استخراج تذكرة منح التذاكر (TGT) الخاصة بالمستخدم داخل المجال، ويفضل أن يكون ذلك من مسؤول المجال. تستهدف هذه التقنية الخبيثة KRBTGT، وهو حساب خدمة موجود في جميع المجالات في Active Directory ويستخدمه مركز توزيع المفاتيح (KDC) ، المسؤول عن إصدار

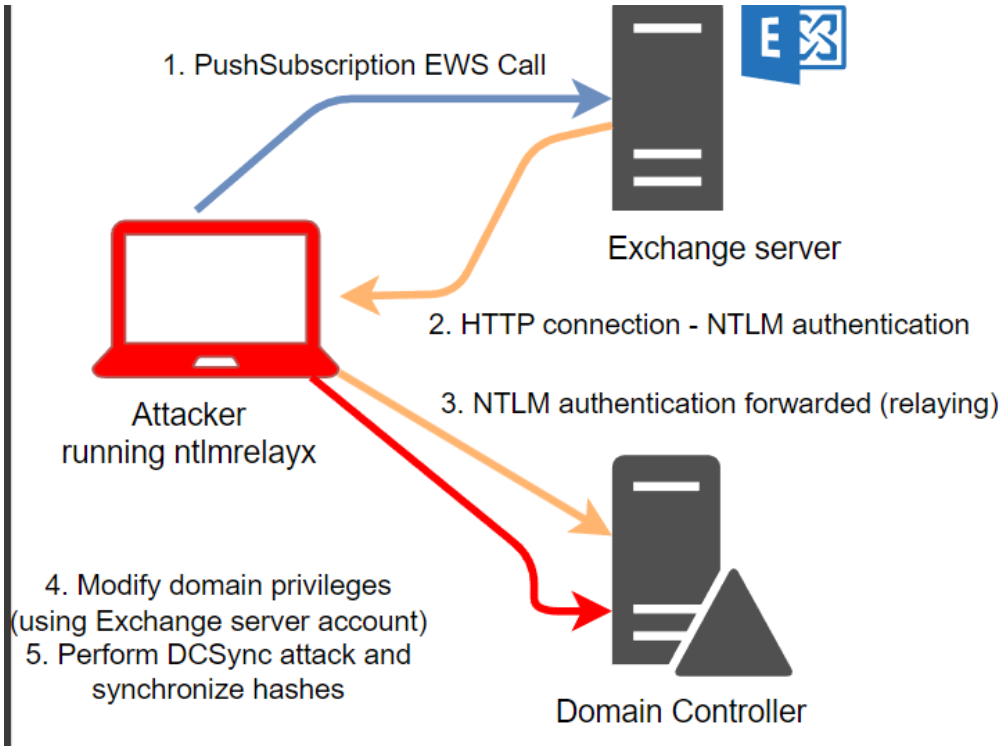
وإدارة تذاكرKerberos، والهدف النهائي هو منح المهاجم وصولاً غير مقيد إلى الشبكة يمكن أن يستمر لمدة تصل إلى 10 سنوات.

SyncDC Attack -3

هجوم SyncDC هو استغلال يستهدف Active Directory ، حيث يتمكن المهاجم من سرقة قاعدة بيانات Active Directory بالكامل، بما في ذلك جميع الحسابات وكلمات المرور. يعتمد الهجوم على آلية النسخ المتماثل التي تُستخدم في Active Directory لضمان تزامن البيانات بين جميع Domain Controllers في الشبكة. المهاجم يقوم بمحاكاة Domain Controller شرعي باستخدام أداة مثل DCSync التي تعد جزءًا من أداة Mimikatz. هذه الأداة ترسل طلبات نسخ متماثل إلى Domain Controller المستهدف، والذي يستجيب بإرسال جميع البيانات المطلوبة مثل كلمات المرور بصيغة Hash، معلومات الحسابات، والمفتاح KRBTGT المستخدم في توقيع تذاكر Kerberos.

لتنفيذ الهجوم، يجب أن يمتلك المهاجم صلاحيات Domain Admin أو ما يعادلها، وهو ما يمكن تحقيقه من خلال هجمات تصعيد الصلاحيات أو سرقة بيانات تسجيل الدخول للحسابات الإدارية. بمجرد الوصول إلى هذه الصلاحيات، يبدأ المهاجم بجمع البيانات، والتي يمكن استغلالها لاحقًا في هجمات مثل Golden Ticket أو فك تشفير كلمات المرور أو انتحال أي حساب على الشبكة. المخاطر الكبرى تكمن في أن الهجوم يمكن أن يمنح المهاجم وصولًا كاملًا ومستمرًا إلى الشبكة، مع صعوبة اكتشافه لأنه يستغل آلية شرعية مدمجة في Active Directory.

لإجراء الهجوم على نظام Kerberos باستخدام أدوات مثل Mimikatz وأداة DCSync، يجب أن يمتلك المهاجم صلاحيات Domain Admin أو ما يعادلها داخل الشبكة، ويمكن الوصول إلى هذه الصلاحيات من خلال هجمات تصعيد الصلاحيات، مثل استغلال الثغرات الأمنية لرفع الامتيازات أو من خلال سرقة بيانات تسجيل الدخول لحسابات إدارية. بمجرد حصول المهاجم على صلاحيات عالية، يقوم باستخدام أداة DCSync، وهي جزء من Mimikatz، والتي تتيح له استغلال بروتوكول النسخ المتماثل الخاص بـ Active Directory. عبر هذه الأداة، يقوم المهاجم بإرسال طلبات نسخ متماثل إلى Domain Controller، مدعيًا أنه Domain Controller آخر، مما يجعله يحصل على معلومات حساسة. بمجرد تنفيذ الطلب، يقوم Domain Controller المستهدف بالرد بإرسال البيانات المطلوبة، والتي تتضمن كلمات مرور المستخدمين بصيغة Hashes مثل (NTLM)، ومعلومات الحسابات (بما في ذلك الحسابات الإدارية)، بالإضافة إلى مفتاح KRBTGT المستخدم في توقيع تذاكر Kerberos. باستخدام هذه البيانات المسروقة، يمكن للمهاجم تنفيذ هجمات متعددة، مثل هجوم Golden Ticket باستخدام مفتاح KRBTGT المسروق، مما يسمح له بإنشاء تذاكر Kerberos مزورة والوصول إلى جميع خدمات الشبكة دون مصادقة إضافية. علاوة على ذلك، يمكن للمهاجم فك تشفير كلمات المرور باستخدام الـ Hashes المسروقة، وانتحال أي حساب مستخدم في الشبكة للحصول على الوصول غير المصرح به إلى الموارد الحساسة. هذه الهجمات تستغل الثغرات في بروتوكول Kerberos و Active Directory مما يعرض الشبكة لخطر كبير في حال تم استغلالها بشكل فعال.



الحصول على صلاحيات عالية (Domain Admin):

لتمكين المهاجم من تنفيذ الهجوم بنجاح، يجب أن يمتلك صلاحيات Domain Admin أو ما يعادلها. يمكن الوصول إلى هذه الصلاحيات من خلال هجمات تصعيد الصلاحيات، مثل استغلال الثغرات الأمنية لرفع الامتيازات أو من خلال سرقة بيانات تسجيل الدخول لحساب إداري. بدون الحصول على هذه الصلاحيات، سيكون من المستحيل تنفيذ الهجمات التالية.

استخدام أداة DCSync:

أداة DCSync هي جزء من أداة Mimikatz وتستغل بروتوكول النسخ المتماثل الخاص بـ Active Directory. يقوم المهاجم باستخدام الأداة لإرسال طلبات نسخ متماثل إلى Domain Controller، مدعيًا أنه Domain Controller آخر. عندما يتم تنفيذ هذا الطلب، يتفاعل Domain Controller المستهدف ويستجيب بإرسال بيانات حساسة يمكن أن يستغلها المهاجم.

جمع البيانات:

بعد إرسال طلبات DCSync، يقوم Domain Controller المستهدف بإرسال البيانات المطلوبة إلى المهاجم، والتي تشمل: كلمات مرور المستخدمين بصيغة Hashes، مثل NTLM، ومعلومات الحسابات، بما في ذلك الحسابات الإدارية.

مفتاح **KRBTGT** المستخدم في توقيع تذاكر Kerberos، والذي يعد من أهم البيانات التي يتمكن المهاجم من استغلالها بشكل لاحق.

استغلال البيانات المسروقة:

بمجرد حصول المهاجم على البيانات المسروقة، يمكنه استخدامها لتنفيذ مجموعة من الهجمات المتقدمة. على سبيل المثال، باستخدام مفتاح KRBTGT المسروق، يمكنه تنفيذ هجوم Golden Ticket، الذي يتيح له إنشاء تذاكر مزورة للوصول إلى جميع خدمات الشبكة دون الحاجة للمصادقة مجددًا. بالإضافة إلى ذلك، يمكنه فك تشفير كلمات المرور باستخدام الـ Hashes المسروقة، أو حتى انتحال هوية أي حساب مستخدم في الشبكة للحصول على وصول غير مصرح به إلى الموارد الحساسة.

:Mimikatz

Mimikatz هي الأداة الأساسية والأكثر شهرة في تنفيذ هجوم Golden Ticket وDCSync .

هي أداة مفتوحة المصدر تستخدم لاستغلال الثغرات الأمنية في أنظمةWindows ، خاصة Active Directoryعبر Mimikatz ، يمكن للمهاجم تنفيذ هجومDCSync ، حيث يقوم بإرسال طلبات DC Sync إلى Domain Controller لاسترجاع بيانات حساسة مثل NTLM hashes وكلمات المرور

الخاصة بالمستخدمين، بالإضافة إلى مفتاح KRBTGT. بمجرد الحصول على مفتاح KRBTGT، يمكن استخدامه لإنشاء Golden Ticket، وهي تذكرة مزورة تسمح للمهاجم بالوصول إلى خدمات Kerberos في الشبكة دون الحاجة إلى المصادقة مجددًا.

PowerShell:

PowerShell يمكن أن يُستخدم لتنفيذ أوامر Mimikatz وDCSync على الخوادم التي قد لا تدعم الأدوات الأخرى أو لتبسيط عملية التنفيذ عبر السكربتات. من خلال PowerShell، يمكن للمهاجم تشغيل Mimikatz لتنفيذ أوامر مثل DCSync أو إنشاء Golden Ticket، مما يتيح له الوصول غير المصرح به إلى الشبكة والخدمات

Netcat:

Netcat هو أداة مفيدة قد يتم استخدامها لتسهيل النقل الآمن للبيانات أو للوصول عن بُعد إلى النظام المستهدف خلال الهجوم. في سياق هجمات Golden Ticket وDCSync، قد يستخدمها المهاجم للاتصال بالخوادم المستهدفة أو لتمرير البيانات بين الأنظمة داخل الشبكة.

BloodHound:

تعد BloodHound أداة تحليل أمان قوية تساعد في تحديد الثغرات في شبكة Active Directory. تستخدم BloodHound لتحليل العلاقات بين الحسابات المختلفة في الشبكة، مما يساعد المهاجمين في اكتشاف الحسابات ذات صلاحيات Domain Admin. هذه المعلومات تعتبر حيوية للمهاجم

لتنفيذ هجمات مثل DCSync و Golden Ticket بشكل فعال، حيث تسهل عملية التصعيد والوصول إلى الحسابات الهامة.

Impacket:

Impacket هي مجموعة من الأدوات التي تستخدم في استغلال الثغرات عبر بروتوكولات SMB و Kerberos في الشبكة. يمكن استخدام Impacket جنبًا إلى جنب مع Mimikatz لتنفيذ الهجمات على Active Directory. فهي توفر للمهاجم الأدوات اللازمة للتفاعل مع Kerberos واختراق الشبكة بسهولة أكبر، مما يسهل عملية تنفيذ هجمات مثل Golden Ticket.

References

1. Kotlaba, L.; Buchovecká, S.; Lórencz, R. Active Directory Kerberoasting Attack: Detection using Machine Learning Techniques.
In Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021), Online, 11–13
February 2021; pp. 376–383.
2. Gkotsis, P. Creating a Windows Active Directory Lab and Performing Simulated Attacks. Master's Thesis, University of Piraeus,
Piraeus, Greece, 2021.
3. Pekta¸s, A.; Ba¸sarano˘ glu, E. Practical Approach For SecuringWindows Environment: Attack Vectors And Countermeasures. In
Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021), Online, 11–13
February 2021; pp. 376–383.
4. Matsuda,W.; Fujimoto, M.; Mitsunaga, T. Detecting apt attacks against active directory using machine learning. In Proceedings
of the 2018 IEEE Conference on Application, Information and Network Security (AINS), Langkawi, Malaysia, 21–22 November
2018; pp. 60–65.
5. Jeun, I.; Lee, Y.; Won, D. A practical study on advanced persistent threats. In Computer Applications for Security, Control and System
Engineering; Springer: Berlin/Heidelberg, Germany, 2012; pp. 144–152.
6. Advanced Persistent Threat (APT) Attacks. Available online: https://www.cynet.com/advanced-persistent-threat-apt-attacks/

(accessed on 30 July 2022).
7. Fireeye Advanced Threat Report 2013: FireEye Labs. 2013. Available online:
https://www2.fireeye.com/rs/fireeye/images/
fireeye-advanced-threat-report-2013.pdf (accessed on 30 July 2022).
8. Quintero-Bonilla, S.; Martín del Rey, A. A new proposal on the advanced persistent threat: A survey. Appl. Sci. **2020**, 10, 3874.
[CrossRef]
9. Kaspersky. Kaspersky's 2019 IT Security Economics Report. Available online: https://go.kaspersky.com/rs/802-IJN-240/
images/GL_Kaspersky_Report-IT-Security-Economics_report_2019.pdf (accessed on 9 September 2021).
10. Steiner, J.G.; Neuman, B.C.; Schiller, J.I. Kerberos: An Authentication Service for Open Network Systems. In Proceedings of the
Usenix Winter, Dallas, Texas, USA, 9–12 February 1988; pp. 191–202.
11. Alva, D.; Benjamin, D. Abusing Microsoft Kerberos. Available online: https://www.blackhat.com/docs/us-14/materials/us-14
-Duckwall-Abusing-Microsoft-Kerberos-Sorry-You-Guys-Don't-Get-It.pdf (accessed on 9 September 2021).
12. Github. BloodHoundAD. Available online: https://github.com/BloodHoundAD/BloodHound (accessed on 13 September 2021).
13. Will Schroeder. PowerSploit. Available online:
https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon (accessed
on 13 September 2021).
14. Cybersecurity Bits, Bobs. Active Directory Domain Enumeration. Available online: https://mlcsec.com/active-directory-domainenumeration/#
(accessed on 13 September 2021).
15. Motero, C.D.; Higuera, J.R.B.; Higuera, J.B.; Montalvo, J.A.S.; Gómez, N.G. On Attacking Kerberos Authentication Protocol in
Windows Active Directory Services: A Practical Survey. IEEE Access **2021**, 9, 109289. [CrossRef]
16. Diogenes, Y.; Ozkaya, E. Cybersecurity—Attack and Defense Strategies: Infrastructure Security with Red Team and Blue Team Tactics;
Packt Publishing Ltd.: Birmingham, UK, 2018.
17. White, S. Net.exe. Available online: https://docs.microsoft.com/en-us/windows/win32/winsock/net-exe-2 (accessed on 13
September 2021).
18. Ebad, S.A. Lessons learned from offline assessment of security-critical systems: the case of microsoft's active directory. Int. J. Syst.
Assur. Eng. Manag. **2022**, 13, 535. [CrossRef]
19. Microsoft. Active Directory. Available online: https://docs.microsoft.com/en-us/powershell/module/activedirectory/?view=
windowsserver2019-ps (accessed on 13 September 2021).
20. Melnick, J. How to Create New Active Directory Users with Powershell, SysAdmin Magazine, June 2019. Available online:
https://blog.netwrix.com/2018/06/07/how-to-create-new-active-directory-users-with-powershell/ (accessed on 13 January
2022).
21. Fletcher, D.R., Jr. Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey. Available online: www.sans.
org/reading-room/whitepapers/analyst/cyber-threat-intelligence-uses-successes-failures-2017-cti-survey-37677 (accessed on
14 March 2017).
22. TNelson; Kettani, H. Open source powershell-written post exploitation frameworks used by cyber espionage groups. In
Proceedings of the 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA,
9–12 March 2020; pp. 451–456.
23. Lemmens, M. BloodHound—Sniffing Out the Path Through Windows Domains. Available online:
https://www.sans.org/blog/
bloodhound-sniffing-out-path-through-windows-domains/ (accessed on 13 September 2021).

24. Myllyla, J.; Costin, A. Reducing the Time to Detect Cyber Attacks: Combining Attack Simulation with Detection Logic. In
Proceedings of the Conference of Open Innovations Association FRUCT (FRUCT Oy, 2021), Oulu, Finland, 27–29 October 2021.
25. Rights, R.F. Use Offense to Inform Defense. Find Flaws before the Bad Guys Do; SANS Institute: Rockville, MD, USA, 2015.
26. El-Hadidi, M.G.; Azer, M.A. Traffic Analysis for Real Time Applications and its Effect on QoS in MANETs. In Proceedings of the
2020 15th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 15–16 December 2020; pp. 1–6. 27. Dimov, D.; Tzonev, Y. Pass-the-hash: One of the most prevalent yet underrated attacks for credentials theft and reuse. In
Proceedings of the 18th International Conference on Computer Systems and Technologies (2017), Ruse, Bulgaria, 23–24 June 2017;
pp. 149–154.
28. Roobol, S.; Offerman, N.; de Laat, C.; van de Wouw, D.; Huijgen, A. Development of Techniques to Remove Kerberos Credentials from
Windows Systems, M.Sc; Security and Network Engineering, School of Computer Science, University of Amsterdam: Amsterdam,
The Netherlands, 2019.
29. Badhwar, R. Advanced Active Directory Attacks and Prevention. In The CISO's Next Frontier; Springer: Midlothian, VA, USA,
2021; pp. 131–144.
30. Ah-Fat, P.; Huth, M.; Mead, R.; Burrell, T.; Neil, J. Effective detection of credential thefts from windows memory: Learning access
behaviours to local security authority subsystem service. In Proceedings of the 23rd International Symposium on Research in
Attacks, Intrusions and Defenses (RAID 2020), San Sebastian, Spain, 14–15 October 2020; pp. 181–194.
31. Higgs, C. Authorisation and Delegation in the Machination Configuration System. LISA **2008**, 8, 191–199.
32. Warren, J. Unconstrained Delegation Permissions. Available online: https://stealthbits.com/blog/unconstrained-delegationpermissions/
(accessed on 10 September 2021).
33. De Clercq, J.; Grillenmeier, G. Microsoft Windows Security Fundamentals: For Windows 2003 SP1 and R2; Elsevier: Amsterdam, The
Netherlands, 2011; ISBN 9780080491882.
34. Amador, M.; Bagwell, K.; Frankel, A. A note on interval delegation. Econ. Theory Bull. **2018**, 6, 239. [CrossRef]
35. Suman, B.; Justin, H. Configuring Kerberos Delegation for Group Managed Service Accounts. Available online: https:
//docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/configure-kerberos-delegationgroup-
managed-service-accounts (accessed on 10 September 2021).
36. Kevin, J. Constrained Delegation Abuse: Abusing Constrained Delegation to Achieve Elevated Access. Available online: https:
//blog.stealthbits.com/constrained-delegation-abuse-abusing-constrained-delegation-to-achieve-elevated-access/ (accessed on
10 September 2021).
37. Markoff, J. Attack of the zombie computers is growing threat. New York Times **2007**, 157, 1.
38. Soria-Machado, M.; Abolins, D.; Boldea, C.; Socha, K. Kerberos golden ticket protection. Mitigating Pass-the-Ticket Act. Dir.
CERT-EU Secur. Whitepaper **2014**, 7, 2016.
39. Metcalf, S. Red vs. Blue: Modern Active Directory Attacks, Detection, & Protection. Available online: https://www.blackhat.com/
docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection.pdf (accessed
on 10 September 2021).
40. Liu, J.; Akhtar, N.; Mian, A. Adversarial training for commonsense inference. IEEE Trans. Neural Netw. Learn. Syst. Rev. **2020**, 47,
777–780.

41. Tramèr, F.; Papernot, N.; Goodfellow, I.; Boneh, D.; McDaniel, P. The space of transferable adversarial examples. arXiv **2017**,
arXiv:1704.03453.
42. Barker, S. White Paper ©; Copyright Quest® Software, Inc.: Aliso Viejo, CA, USA, 2007.
43. Boger, T. Directory Services Restore Mode (DSRM), & Protection. Available online:
https://searchwindowsserver.techtarget.com/
definition/Directory-Services-Restore-Mode-DSRM (accessed on 13 September 2021).
44. Warren, J. Stealing Credentials with a Security Support Provider (SSP). Available online:
https://stealthbits.com/blog/stealingcredentials-
with-a-security-support-provider-ssp/ (accessed on 13 September 2021).
45. Jacobs, M.; Satran, M. How Access Control Works in Active Directory Domain Services. Available online:
https://docs.microsoft.
com/en-us/windows/win32/ad/how-access-control-works-in-active-directory-domain-services (accessed on 13 September
2021).
46. Metcalf, S. Sneaky Active Directory Persistence #15: Leverage AdminSDHolder & SDProp to (Re)Gain Domain Admin Rights.
Available online: https://adsecurity.org/?p=1906 (accessed on 13 September 2021).
47. Mittal, N.; RACE—Minimal Rights and ACE for Active Directory Dominance. Available online:
http://www.labofapenetrationtester.
com/2019/08/race.html (accessed on 13 September 2021).
48. Wheeler, S.;Wilson, C. Running Remote Commands. Available online: https://docs.microsoft.com/en-us/powershell/scripting/
learn/remoting/running-remote-commands?view=powershell-7 (accessed on 13 September 2021).
49. Nichols, J.A.; Taylor, B.A.; Curtis, L. Security resilience: Exploring windows domain-level defenses against post-exploitation
authentication attacks. In Proceedings of the 11th Annual Cyber and Information Security Research Conference (2016), Oak
Ridge, TN, USA, 5–7 April 2016; pp. 1–4.
50. Jadeja, N.; Vaghasia, M. Analysis and Impact of Different Mechanisms of Defending Pass-the-Hash Attacks. In Cyber Security;
Springer: Singapore, 2018; pp. 179–191.
51. Binduf, A.; Alamoudi, H.O.; Balahmar, H.; Alshamrani, S.; Al-Omar, H.; Nagy, N. Active directory and related aspects of security.
In Proceedings of the 2018 21st Saudi Computer Society National Computer Conference (NCC) (IEEE, 2018), Riyadh, Saudi
Arabia, 25–26 April 2018; pp. 4474–4479. 52. Fujimoto, M.; Matsuda,W.; Mitsunaga, T. Detecting Abuse of Domain Administrator Privilege UsingWindows Event Log. In
Proceedings of the 2018 IEEE Conference on Application, Information and Network Security (AINS), Langkawi, Malaysia, 21–22
November 2018; pp. 15–20.
53. Liu, Y.; Squires, M.R.; Taylor, C.R.; Walls, R.J.; Shue, C.A. Account Lockouts: Characterizing and Preventing Account Denial-of-
Service Attacks. In Proceedings of the International Conference on Security and Privacy in Communication Systems, Orlando, FL,