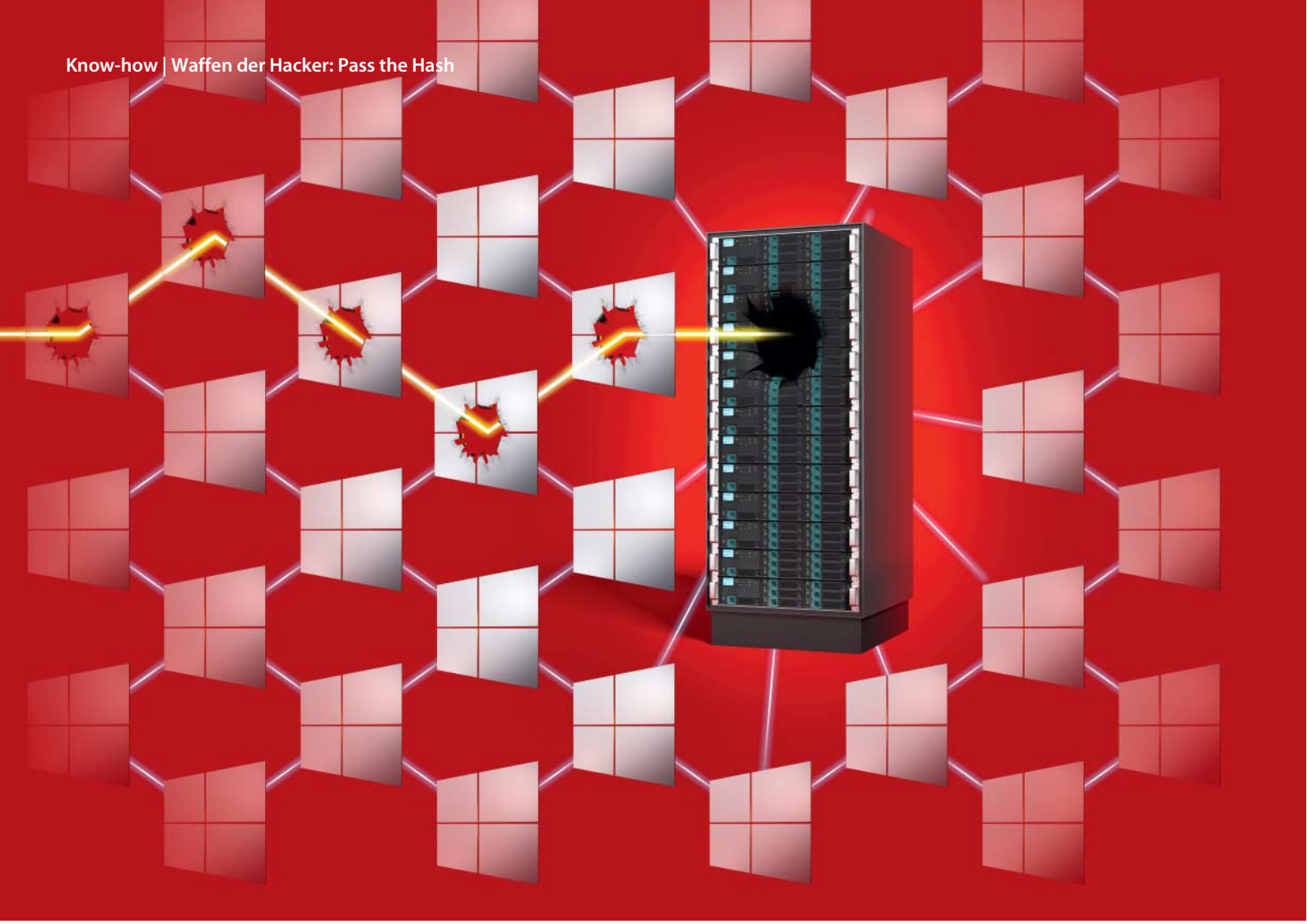


Oliver Klarmann, Jürgen Schmidt

Hash mich, ich bin der Admin

Pass the Hash als Gefahr für Windows-Netze

Ambitionierten Angreifern reicht es nicht, den Rechner eines Sachbearbeiters mit einem Flash-Exploit zu kapern. Die wollen die E-Mails des CEO lesen und die wichtigen Server im Netz kontrollieren. Da sind oft Pass-the-Hash-Angriffe das Mittel ihrer Wahl.

Exploits kommen auch bei gezielten Angriffen zum Einsatz, etwa zum Ausspähen von Firmengeheimnissen oder zur Sabotage via Internet. Auf diesem Weg landet der Angreifer aber kaum auf einem zentralen Server mit wichtigen Daten oder einem System zur Steuerung der anvisierten Anlage. Eher findet er sich nach einem erfolgreichen Angriff auf dem Arbeitsplatzrechner einer Sekretärin wieder, die der gut gemachten Phishing-Mail nicht widerstehen konnte.

Von hier aus steht der Angreifer vor der Aufgabe, sich im Netz der attackierten Firma weiterzuhangeln, bis er Zugang zum eigentlichen Ziel erlangt. Wie das im Einzelnen passiert, hängt von den Gegebenheiten ab, die er vorfindet. Eine bewährte Methode, sich zum uneingeschränkten Herrscher eines Windows-Netzes aufzuschwingen, ist der Pass-the-Hash-Angriff – kurz PtH.

Diese Technik nutzten etwa die Anunak-Bankräuber, um 2014 bei Banken in über zwanzig Ländern über eine Milliarde US-Dollar zu erbeuten. Wie üblich drangen sie zunächst über den Rechner eines einfachen Bankangestellten in das Netz ein. Dann verschafften sie sich von dort aus via Pass-the-Hash-Attacken Zugang zu einem Adminstrator-Konto mit Zugriff auf die eigentlichen Banking-Systeme, auf denen sie dann gekonnt Geld umleiteten.

Mehrere Faktoren machen Pass-the-Hash-Angriffe besonders bedrohlich: Die Methode verleiht dem Angreifer potenziell unbeschränkte Macht im Windows-Netz. Er kann damit beliebige Accounts kapern – einschließlich dem eines Domänen-Administrators. Darüber kann er dann beliebig auf Server und Anwender-Daten im Windows-Netz zugreifen.

Es gibt bereits fertige Tools, mit denen sich ganz reale Angriffe umsetzen lassen. Diese sind frei im Internet verfügbar; die Anunak-Gang etwa verwendete für ihre Raubzüge eine angepasste Version des Open-Source-

Tools Mimikatz. Das Modul psexec im universellen Angriffs-Framework Metasploit führt übers Netz beliebige Befehle auf anderen Windows-Rechnern aus und setzt dabei die Pass-the-Hash-Technik ein.

Und schließlich ist es fast unmöglich, sich vollständig vor diesen Angriffen zu schützen. Sicherheits-Tester berichten, dass sie in über 90 Prozent der Windows-Netze mit Pass-the-Hash-Angriffen Erfolg haben.

Das liegt daran, dass diese Angriffsform nicht auf einer Sicherheitslücke beruht, die man mit einem Update schließen könnte, sondern auf einem Design-Problem von Windows-Netzen. Dieses Problem der Windows-Authentifizierung ist seit Jahren bekannt und es wird dazu keinen Patch geben. Stattdessen verweist Microsoft auf Maßnahmen, die Gefahr zu reduzieren und den Aufwand für den Angreifer zu erhöhen.

Das Problem

Das Design-Problem ist auf das Windows-Konzept einer zentralen Anmeldung an alle Dienste zurückzuführen. Ein Kennwort genügt, um sich überall im Netz auszuweisen und auf alle Dienste zuzugreifen. Man authentisiert sich mit der ersten Anmeldung einmal am System und wird künftig nicht mehr nach Benutzername und Passwort gefragt. Dies gilt unabhängig von der genutzten Ressource, also egal ob Outlook/Exchange, SharePoint, Datei- oder Druckserver.

Ein Passwort ist nicht mehr so einfach wie früher zu klauen, denn es liegt normalerweise nirgends im Klartext rum und wird auch nicht mehr im Klartext durch das Netz verschickt. Stattdessen kommen sogenannte Hashes zum Einsatz.

Zum Anmelden an einen Dienst wendet der Client zunächst eine Hash-Funktion auf das Passwort an und schickt dann diesen Hash-Wert an den Server. Der vergleicht ihn mit dem dort gespeicherten Hash und gewährt bei Übereinstimmung den gewünschten Zugang. Der Vorteil dieses Verfahrens: Wer den Hash-Wert erlauscht, kann daraus das Passwort nicht zurückrechnen. Das muss er aber auch gar nicht.

Denn die Anmeldung an den meisten Windows-Diensten erfordert gar kein Passwort. Ein Angreifer muss also nicht auf veraltete LM- oder NTLMv1-Hashes hoffen, die er leicht knacken kann. Es genügt vollkommen, wenn er sich einen aktuellen NTLMv2-Hash besorgt und diesen direkt zur Anmeldung vorweist. Dazu muss er nur die jeweilige Client-Software so modifizieren, dass sie den Hash-Vorgang weglässt und den übergebenen Hash-Wert direkt an den Server weitergibt: „Pass the Hash!“ Im Prinzip öffnet dieser Hash dann den Zugang zu allem, was mit „Single Sign On“ funktioniert.

Give me the Hash

Es stellt sich die Frage, wo ein Angreifer solche Hash-Werte herbekommt. Es bieten sich erschreckend viele Möglichkeiten, diese Werte abzugreifen. Windows speichert die NT LAN Manager Hashes – kurz NTLM-Hashes – in der Datenbank des Security Accounts Manager (SAM) auf der Festplatte. Allerdings liegen dort nur die Daten der lokalen Benutzer; ein Tool wie pwdump spuckt also lediglich die Hashes lokaler Benutzerkonten aus, die im Netz nicht funktionieren. Für die Anmeldung im Netz benötigt man die NTLM-Hashes der Netzwerk-Identitäten, die der Domänen-Controller in seiner Active-Directory-Datenbank verwaltet.

Hacking-Tools wie der Windows Credentials Editor (WCE) durchsuchen auch den Arbeitsspeicher des Systems nach solchen Hashes. Und da wird es spannend: Wenn sich ein Anwender im Netz anmeldet, hält Windows seinen NTLM-Hash im Arbeitsspeicher vor, damit es zum gewünschten Single-Sign-On alle weiteren Authentifizierungs-Anforderungen ohne Rückfrage beim Benutzer erledigen kann.

Konkret liegen die NTLM-Hashes im Arbeitsspeicher des Local Security Authority Subsystem Service (LSASS). Sprich: WCE spuckt auch die NTLM-Hashes aller auf dem System gerade angemeldeten Netzwerk-Benutzer aus. Das funktioniert bei nahezu allen Windows-Versionen; erst in den noch nicht sonderlich weit verbreiteten Windows 8.1 und Windows Server 2012 R2 hat Microsoft spezielle Vorkehrungen eingebaut, die diesen Zugriff zumindest deutlich erschweren.

Ein durchaus realistisches Szenario ist das eines Admins, der sich etwa zur Installation von Software via Remote-Desktop-Protokoll (RDP) auf dem Rechner eines Sachbearbeiters anmeldet. Dabei landet der NTLM-Hash des Domänen-Admins im RAM des Arbeitsplatzrechners. Und wenn der Admin sich – wie durchaus üblich – via Disconnect abmeldet, verbleibt er dort sogar zunächst. Erst ein echter Neustart des Arbeitsplatzrechners oder eine reguläre Abmeldung von der RDP-Sitzung löscht den Hash-Wert zuverlässig aus dem Speicher.

Gelangt ein Angreifer also über einen Exploit auf den Rechner dieses Sachbearbeiters, kann er den NTLM-Hash des Domänen-Admins aus dem RAM des Arbeitsplatzrechners fischen. Mit etwas Glück befindet sich der noch im Speicher. Andernfalls inszeniert er eben ein kleines Problem, das den Admin erneut auf den Plan ruft. Verwendet der Admin das gleiche Konto für seine anderen administrativen Tätigkeiten, was durchaus gang und gäbe ist, dann ist der Hacker bereits am Ziel. Künftig kann er mit dem von WCE erschnüffelten NTLM-Hash als Domain-Admin im Netz schalten und walten.

Neben den Domain-Admin-Hashes gibt es eine ganze Reihe weiterer lohnender Ziele für Pass-the-Hash-Angriffe. Vor allem netzwerkweit eingesetzte Dienste sind interessant. Wenn sich etwa der Backup-Agent mit seinen weitreichenden Leseberechtigungen auf allen Systemen mit dem gleichen NTLM-Hash ausweist, bedeutet das freie Fahrt für den PtH-Spion.

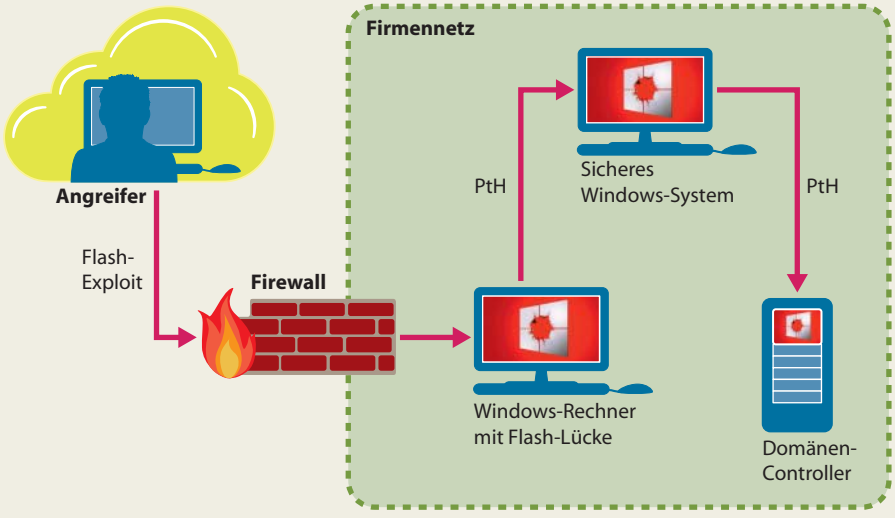
Privilegien

Eine Hürde muss der Angreifer vor einem erfolgreichen Pass-the-Hash-Angriff allerdings noch nehmen, die bislang nicht erwähnt wurde: In Firmen arbeiten die Mitarbeiter in aller Regel nur mit eingeschränkten Benutzer-Konten; der Zugriff auf den SAM und erst recht auf das RAM erfordert aber System-Rechte.

Ein herkömmlicher Exploit, etwa über eine Sicherheitslücke in Flash, beschert dem Angreifer maximal die Zugriffsrechte des angemeldeten Benutzers – also im Normalfall ohne Zugang zu SAM und RAM.

Angriff auf Windows-Netze

Mit der Pass-the-Hash-Methode (PtH) hangelt sich der Angreifer durchs Firmen-Netz und kapert schließlich sogar den Domänen-Controller.



Schutzmaßnahmen

- Sicherung des Netzwerks gegen Eindringlinge (Updates, Patches, Firewall, Proxy-Server, Virenscanner, IDS)
- unterschiedliche Admin-Konten für Arbeiten am Server und den PCs
- sauberes Abmelden von RDP-Sitzungen oder anderen Zugriffen wie Admin-Freigaben von PCs
- eigene (beschränkte) Benutzerkonten für Dienste wie Backup-Software
- eigene (beschränkte) Benutzerkonten für zeitgesteuerte Aufgaben
- Sperren der Zugriffe von Clients auf Server(dienste), wo immer möglich
- regelmäßige Kennwortänderungen auch von Administrativen- und Dienst-Konten
- zusätzliche Verschlüsselung aller (wichtigen) Daten

Das bedeutet, dass sich der Hacker zunächst volle Systemrechte verschaffen muss – Profis sprechen von Local Privilege Escalation. Auch hier gilt, dass sich das in der Praxis sehr schwer verhindern lässt. Schon die Zahl der immer wieder bekannt werdenden Local-Privilege-Escalation-Lücken zeigt, dass man da kein einzelnes Loch zu stopfen hat, sondern eher ein Sieb.

Ambitionierte Hacker-Crews haben spezielle Zero-Day-Explots zur Ausweitung ihrer Rechte zum Admin- oder Systemkonto parat. Googles Project Zero veröffentlichte in den letzten Monaten allein zwei solcher Local-Privilege-Escalation-Probleme in Windows, die Microsoft wohl gar nicht beseitigen wird, weil das zu tiefe Eingriffe in das System erfordert.

Oft braucht es jedoch gar keine 0-Days, um Systemrechte zu erlangen. Es genügt ein einziges Programm, das bei der Installation mit der Vergabe der Rechte etwas zu großzügig war und beispielsweise Schreibzugriffe auf die Konfiguration oder sogar die ausführbare Datei eines Dienstes erlaubt. Tools wie AccessChk aus der Sysinternals-Suite scannen den kompletten Rechner und decken solche Lücken gnadenlos auf.

Weitere Angriffsziele sind Backup-Dienste, Software-Verteilung und andere administrative Dienste, die mit hohen Rechten laufen, aber oft nicht wasserdicht konfiguriert sind. Zusammengefasst: Die Arbeit mit eingeschränkten Benutzerkonten und ein Forcieren dieser Beschränkung ist eine sehr gute Prävention gegen viele Angriffsszenarien, auch gegen PtH-Attacken. Sich darauf zu verlassen, dass man auf diesem Weg Pass-the-Hash-Angriffe in seinem Netz komplett verhindern könnte, wäre jedoch fatal.

PtH in der Praxis

Das ganze Angriffsszenario ist keineswegs eine Chimäre. Im Rahmen der heise-Security-Tour im Mai zeigte Referent Philipp Buchegger live vor Publikum, wie er mit WCE das Konto eines Domain-Admins kapern konnte. Wir haben für diesen Artikel in zwei Umgebungen PtH-Attacken konkret gestestet. Zuerst in einer Sandkasten-Umgebung mit einem Windows Server 2008 R2 Domänen-Controller, einem weiteren 2008 R2 als Member-Server sowie Windows 7 Professional x64 als Client. Der zweite Test fand mit dem alten Produktiv-Server des Autors statt – einem Small Business Server 2003 und ebenfalls einem Windows-7-Client. Der SBS 2003 befindet sich immer noch vielfach im Einsatz.

Zunächst war es erforderlich, den eingesetzten Windows Credential Editor (WCE) am Virenscanner vorbeizuschmuggeln. Erkannte dieser das Tool, löschte er es noch vor dem ersten Start. Doch diese Hürde kann ein motivierter Angreifer ohne große Probleme nehmen. Danach funktionierte WCE wie beschrieben: Er spuckte unter anderem die Hashes der übers Netz angemeldeten Benutzer aus, mit denen es möglich war, Sitzungen mit deren Benutzerkennung zu starten, um zum Beispiel auf Dateifreigaben zuzugreifen.

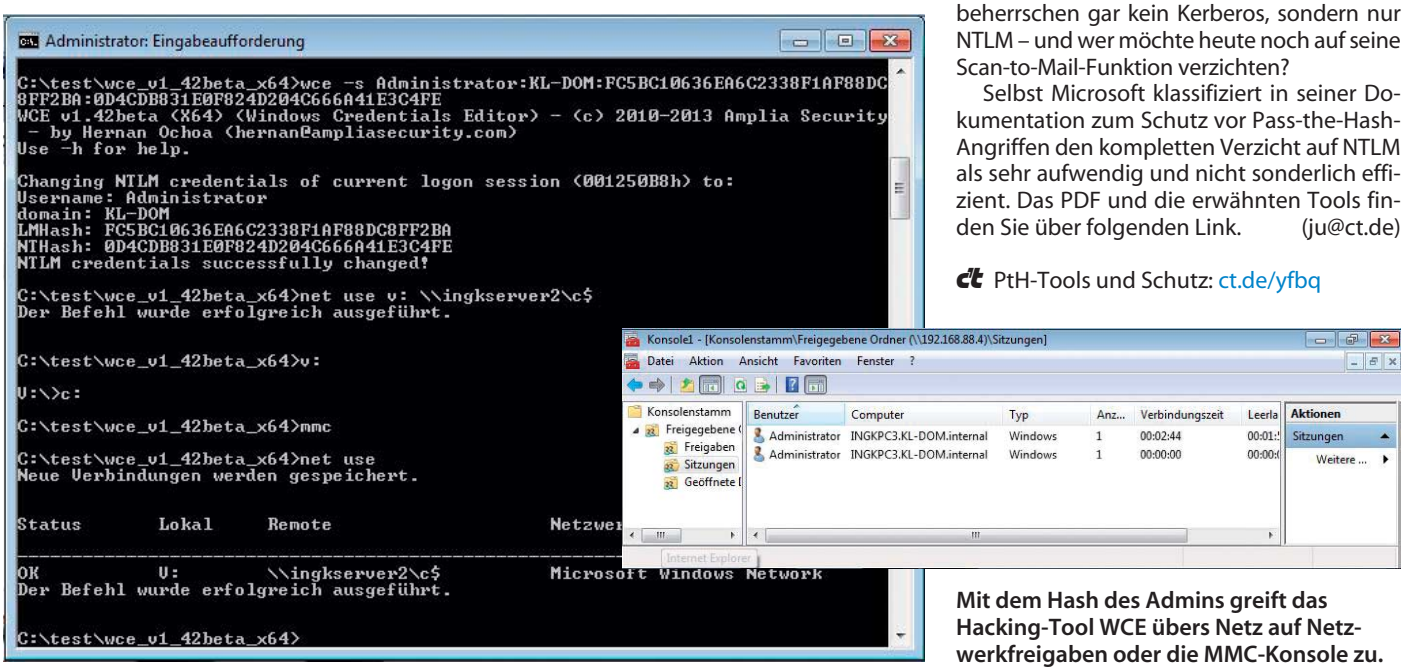
Eine Möglichkeit, Pass-the-Hash-Angriffe unmöglich zu machen, besteht darin, NTLM komplett auszumustern. Im Prinzip ist das durchaus machbar. Denn es gibt bereits einen Nachfolger, der NTLM im Active Directory ablösen soll: Kerberos. In der Windows-Netzwerk-Welt ist das sogar seit vielen Jahren das Standard-Authentifizierungsverfahren. Dabei handelt es sich um ein Ticket-basiertes System, bei dem sich ein Client für den Zugang zu einem Dienst vom Kerberos-Server ein Ticket ausstellen lässt.

Anders als NTLM-Hashes, die unbegrenzt für alle Dienste und ohne zeitliche Beschränkung gültig sind, gilt ein Kerberos-Ticket nur für diesen einen Dienst und nur für begrenzte Zeit. Zwar gibt es gegen Kerberos Pass-the-Ticket-Angriffe und Attacken auf Basis von sogenannten Golden oder Silver Tickets, die zum Erstellen weiterer Tickets berechtigen. Doch diese Angriffe sind deutlich schwieriger durchzuführen als Pass-the-Hash.

Das Problem liegt an einer anderen Stelle: Kerberos ist kein vollwertiger Ersatz für NTLM. Deshalb kommt in nahezu allen Windows-Netzen immer noch NTLM zum Einsatz – und sei es nur als Fallback. Das fängt damit an, dass für Kerberos ein Active Directory zwingend erforderlich ist. Gibt es das nicht, bleibt nur NTLM. Kann die Situation eintreten, dass der Domänen-Controller nicht erreichbar ist, überbrücken gecachte NTLM-Credentials diesen Ausfall. Viele Geräte wie Multifunktionsdrucker beherrschen gar kein Kerberos, sondern nur NTLM – und wer möchte heute noch auf seine Scan-to-Mail-Funktion verzichten?

Selbst Microsoft klassifiziert in seiner Dokumentation zum Schutz vor Pass-the-Hash-Angriffen den kompletten Verzicht auf NTLM als sehr aufwendig und nicht sonderlich effizient. Das PDF und die erwähnten Tools finden Sie über folgenden Link. (ju@ct.de)

c't PtH-Tools und Schutz: ct.de/yfbq



Mit dem Hash des Admins greift das Hacking-Tool WCE übers Netz auf Netzwerkfreigaben oder die MMC-Konsole zu.