Faszination Cybercrime

Das umfassende
Cybercrime & -security
Kompendium

Band 2

P bis Z

Klaus-Peter Baumdick

2024

Klaus-Peter Baumdick
c/o COCENTER
Koppoldstr. 1
86551 Aichach

Text: Libreoffice Writer 7.3.4.2

Coverdesign: Klaus-Peter Baumdick

Grafik: aitubo.ai

Erste Auflage

ISBN: 978-3-384-27243-0

Inhaltsverzeichnis

Pass-the-Hash-Angriff

Ein Pass-the-Hash (PtH)-Angriff ist eine Technik, die von Angreifern verwendet wird, um sich in einem Netzwerk zu bewegen und Zugang zu Ressourcen zu erlangen, ohne dass sie das Klartext-Passwort eines Benutzers kennen müssen. Stattdessen verwenden sie den kryptografischen Hash eines Passworts, um sich als der entsprechende Benutzer auszugeben. Dieser Angriff ist besonders relevant in Umgebungen, die auf Microsoft Windows basieren, da dort NTLM (NT LAN Manager) Authentifizierungsprotokolle verwendet werden, die anfällig für diese Art von Angriff sind.

Wie funktioniert ein Pass-the-Hash-Angriff?

1. Erfassen des Hashes:

- Der Angreifer muss zuerst den Hash des Passworts eines Benutzers erfassen. Dies kann durch verschiedene Methoden erfolgen, wie z.B.:

- Credential Dumping: Tools wie Mimikatz können verwendet werden, um Passwort-Hashes aus dem Speicher eines kompromittierten Systems zu extrahieren.

- MitM-Angriffe: Man-in-the-Middle-Angriffe oder andere Netzwerktechniken können genutzt werden, um Hashes während der Übertragung zu erfassen.

2. Verwenden des Hashes:

- Nachdem der Hash erfasst wurde, verwendet der Angreifer diesen Hash, um sich gegenüber anderen Systemen als der legitime Benutzer zu authentifizieren. Der Hash wird in den Authentifizierungsprozess eingespeist, als wäre es das eigentliche Passwort.

3. Bewegung im Netzwerk:

- Mit dem Hash kann der Angreifer auf verschiedene Ressourcen zugreifen, wie z.B. Dateien, Datenbanken und andere Systeme im Netzwerk, die denselben Hash zur Authentifizierung verwenden. Dieser Schritt wird oft als "laterale Bewegung" bezeichnet.

Beispiel eines Pass-the-Hash-Angriffs

1. Kompromittierung eines Workstations:

- Der Angreifer kompromittiert eine Workstation und führt ein Tool wie Mimikatz aus, um NTLM-Hashes aus dem Speicher zu extrahieren.

2. Extrahieren des Hashes:

- Der Angreifer extrahiert den Hash eines Administrator-Kontos oder eines anderen privilegierten Benutzers.

3. Benutzen des Hashes:

- Der Angreifer verwendet den erlangten Hash, um sich auf anderen Maschinen im Netzwerk als dieser Benutzer zu authentifizieren, ohne das tatsächliche Passwort zu kennen.

4. Zugriff auf Ressourcen:

- Der Angreifer bewegt sich lateral durch das Netzwerk, greift auf sensible Daten zu oder führt weitere Angriffe durch, wie z.B. das Installieren von Malware oder das Erstellen von Backdoors.

Schutzmaßnahmen gegen Pass-the-Hash-Angriffe

1. Verwendung von Kerberos:

- Wo möglich, Kerberos anstelle von NTLM verwenden, da Kerberos sicherer ist und weniger anfällig für Pass-the-Hash-Angriffe.

2. Einschränkung von Privilegien:

- Minimieren der Anzahl von Benutzerkonten mit administrativen Rechten und Verwendung von Privileged Access Management (PAM), um den Zugriff zu kontrollieren.

3. Sichere Konfigurationen und Patching:

- Sicherstellen, dass Systeme und Anwendungen stets auf dem neuesten Stand sind, um Sicherheitslücken zu schließen, die zur Hash-Erfassung genutzt werden könnten.

4. Verwendung von multifaktorieller Authentifizierung (MFA):

- Implementierung von MFA, um die Authentifizierung nicht nur von einem Passwort oder Hash abhängig zu machen.

5. Netzwerksegmentierung:

- Segmentierung des Netzwerks, um zu verhindern, dass ein kompromittiertes Konto Zugang zu kritischen Systemen im gesamten Netzwerk erhält.

6. Überwachung und Erkennung:

- Einsatz von Monitoring-Tools und Intrusion Detection Systems (IDS), um verdächtige Aktivitäten zu erkennen, die auf einen Pass-the-Hash-Angriff hinweisen könnten.

Pass-the-Ticket-Angriff

Ein Pass-the-Ticket (PtT)-Angriff ist eine Methode, die von Angreifern verwendet wird, um Zugang zu einem Netzwerk zu erhalten, indem sie gestohlene Ticket-Dateien (normalerweise Kerberos-Tickets) verwenden, um sich als legitimer Benutzer auszugeben. Ähnlich wie bei Pass-the-Hash-Angriffen werden hierbei kryptografische Artefakte wie Kerberos-Tickets ausgenutzt, um unberechtigten Zugriff zu erlangen.

Funktionsweise eines Pass-the-Ticket-Angriffs:

1. Erfassen der Ticket-Datei:

- Der Angreifer muss zuerst Zugriff auf die Ticket-Datei eines legitimen Benutzers erhalten. Diese Dateien enthalten kryptografische Token, die von einem Authentifizierungsserver (normalerweise ein Domain Controller) ausgestellt wurden.

2. Weitergabe des Tickets:

- Nachdem die Ticket-Datei erfasst wurde, verwendet der Angreifer sie, um sich gegenüber anderen Diensten oder Systemen im Netzwerk als der legitime Benutzer auszugeben. Dies ermöglicht es dem Angreifer, auf Ressourcen zuzugreifen, für die der legitime Benutzer berechtigt ist.

3. Ausnutzung von Berechtigungen:

- Durch die Verwendung des gestohlenen Tickets kann der Angreifer auf Ressourcen zugreifen, die für den legitimen Benutzer zugänglich sind. Dies kann sensible Daten, Systemadministrationsrechte oder andere privilegierte Funktionen umfassen.

Beispiel eines Pass-the-Ticket-Angriffs:

1. Erfassen eines Ticket-Granting Tickets (TGT):

- Der Angreifer erlangt Zugriff auf die Ticket-Datei eines Benutzers, die ein Ticket-Granting Ticket (TGT) enthält, das normalerweise vom Key Distribution Center (KDC) ausgestellt wurde.

2. Weitergabe des TGTs:

- Der Angreifer verwendet das TGT, um Zugriff auf andere Dienste oder Ressourcen im Netzwerk zu erhalten. Er gibt sich als der legitime Benutzer aus, für den das TGT ausgestellt wurde.

3. Zugriff auf Ressourcen:

- Durch die erfolgreiche Weitergabe des Tickets kann der Angreifer auf Ressourcen zugreifen, die für den legitimen Benut-

zer zugänglich sind, wie z.B. Dateien, Anwendungen oder Netzwerkressourcen.

Schutzmaßnahmen gegen Pass-the-Ticket-Angriffe:

1. Monitoring und Auditierung:

- Überwachen Sie das Netzwerk auf verdächtige Aktivitäten, die auf den Missbrauch von Tickets hinweisen könnten, und protokollieren Sie alle Authentifizierungsereignisse.

2. Einsatz von Endpunkt-Sicherheitslösungen:

- Implementierung von Sicherheitslösungen auf Endpunkten, die das Abfangen und die Weitergabe von Ticket-Dateien erkennen können.

3. Sichere Konfiguration von Diensten:

- Konfigurieren Sie Dienste und Anwendungen so, dass sie die Verwendung von Tickets streng überwachen und verdächtige Aktivitäten blockieren oder alarmieren.

4. Regelmäßiges Patchen und Updates:

- Halten Sie alle Systeme und Anwendungen auf dem neuesten Stand, um Sicherheitslücken zu schließen, die von Angreifern ausgenutzt werden könnten, um Tickets zu stehlen.

5. Least Privilege-Prinzip:

- Beschränken Sie die Berechtigungen von Benutzern und Diensten auf das absolute Minimum, das für die Ausführung

ihrer Aufgaben erforderlich ist, um das Potenzial für Missbrauch zu reduzieren.

6. Verwendung von Verschlüsselung:

- Implementierung von Verschlüsselungstechniken, um die Sicherheit von Ticket-Dateien während der Übertragung zu gewährleisten und das Risiko des Abfangens durch Angreifer zu verringern.

Paros Proxy

Paros Proxy ist ein Tool, das für Sicherheitsanalysen und Penetrationstests von Webanwendungen verwendet wird. Es fungiert als Man-in-the-Middle (MitM)-Proxy, der den Datenverkehr zwischen dem Client und der Webanwendung abfängt und analysiert. Hier sind die Hauptmerkmale und typischen Anwendungsfälle von Paros Proxy:

1. Man-in-the-Middle (MitM)-Angriffe. Paros Proxy ermöglicht es einem Sicherheitsforscher oder Penetrationstester, als Proxy-Server zwischen dem Client und der Webanwendung zu agieren. Dadurch kann der Datenverkehr überwacht, manipuliert und analysiert werden.

2. HTTP- und HTTPS-Unterstützung. Das Tool unterstützt sowohl unverschlüsselte HTTP- als auch verschlüsselte HTTPS-Verbindungen, wodurch es möglich ist, auch den verschlüsselten Datenverkehr zwischen Client und Server zu analysieren.

3. Session Recording und Wiedergabe. Paros Proxy kann Sitzungen aufzeichnen, einschließlich der HTTP- und HTTPS-Anfragen und -Antworten, die zwischen dem Client und der Webanwendung ausgetauscht werden. Diese Aufzeichnungen können später zur Analyse oder Wiedergabe verwendet werden.

4. Webanwendungs-Sicherheitsscanner. Es enthält Funktionen zur automatisierten Schwachstellenanalyse von Webanwendungen, einschließlich SQL-Injection, Cross-Site Scripting (XSS) und anderen Sicherheitslücken.

5. Interaktive Manipulation des Datenverkehrs. Paros Proxy erlaubt es dem Benutzer, den HTTP- und HTTPS-Datenverkehr in Echtzeit zu manipulieren, indem Anfragen geändert oder gesendet werden, um das Verhalten der Webanwendung zu testen und Schwachstellen zu identifizieren.

6. Berichterstellung. Es bietet Funktionen zur Erstellung von Berichten über gefundene Sicherheitslücken und Schwachstellen, die in der Webanwendung entdeckt wurden.

Typische Anwendungsfälle

1. Sicherheitsbewertung von Webanwendungen. Sicherheitsforscher und Penetrationstester verwenden Paros Proxy, um Schwachstellen in Webanwendungen zu identifizieren und zu analysieren, einschließlich Sicherheitslücken wie SQL-Injection, XSS und Cross-Site Request Forgery (CSRF).