Security Lab – Password-Cracking

VMware

Dieses Lab müssen Sie mit dem **Kali Linux-Image** durchführen.

1 Einleitung

In diesem Praktikum werden Sie verschiedene Methoden für das Offline Password-Cracking kennenlernen und anwenden, um Systempasswörter und die verwendeten Passwörter in einem Challenge-Response-basierten Authentisierungsprotokoll zu knacken.

2 Einführung in Passwort-Hashing

Zu dem Zeitpunkt, zu dem Sie dieses Lab bearbeiten, haben wir Hashfunktionen und ihre Rolle bei der Speicherung von Passwörtern noch nicht durchgenommen. Glücklicherweise wird für dieses Lab keine detaillierte Kenntnis über Hashfunktionen benötigt, nur ein paar Grundresultate und ein Modell. Wir starten mit dem Modell.

Stellen Sie sich eine Kiste vor, in der zwei Löcher sind. In das eine Loch können Sie *beliebig lange Bitstrings irgendeiner Art hineintun*, die man *Urbilder* (engl. *preimage*) nennt, und aus dem anderen Loch kommt *ein Bitstring fester Länge* (z.B. 256 bit) *heraus*, den man *Hash* nennt. Wenn Sie *dieselben Bitstrings hineintun, kommt derselbe Bitstring heraus*. Wenn Sie *verschiedene Bitstrings hineintun*, kommen Bitstrings heraus, die *weder untereinander noch mit den Eingaben irgendetwas zu tun haben*. Echte kryptographische Hashfunktionen verhalten sich wie diese Kiste. Beachten Sie aber, dass es sich hier nur um ein *Modell* handelt, also um eine Art, wie man über Hashfunktionen nachdenken kann. Realisiert werden solche Funktionen anders. Ist x ein preimage und h der zugehörige Hash der Hashfunktion H, dann schreibt man $h = H(x)$.

Kryptographische Hashfunktionen haben ein paar Eigenschaften. Diese hier brauchen wir für das Praktikum:

1. Aus einem Hash kann man kein preimage leicht berechnen. Ist also $h = H(x)$ gegeben, ohne dass man x kennt, ist man aufgeschmissen. Man nennt das *preimage-Resistenz.*
2. Natürlich lässt sich zu einem gegebenen Hash h ein Urbild durch Ausprobieren herstellen: man versucht so lange verschiedene x, bis man eines findet, für das $h = H(x)$ gilt. Sind alle möglichen Urbilder gleichwahrscheinlich, gilt: Bei einer Hashfunktion, die Hashes von n bit Länge produziert, muss man im Mittel 2^n Hashes berechnen, um ein Urbild auf diese Art zu finden. Wenn n gross genug ist, stehen Punkt 1 und 2 also nicht in Widerspruch.

Was hat das nun mit der Speicherung von Passwörtern zu tun? Wenn ich mich bei einem System anmelden möchte, das Passwörter für die Authentifikation nutzt, übermittle ich bei der Anmeldung meinen Benutzernamen und mein Passwort. Das System prüft dann, ob es einen Benutzer mit dieser Benutzername/Passwort-Kombination gibt. Ist das der Fall, wird die Person angemeldet, ansonsten nicht.

Um die Prüfung vornehmen zu können, muss das System irgendwie entscheiden können, ob das von mir übermittelte Passwort richtig ist. Eine einfache Möglichkeit besteht darin, eine Datei auf dem System zu führen, in der alle gültigen Benutzername/Passwort-Kombinationen verzeichnet sind. Gelangt aber ein Angreifer in den Besitz dieser Datei, besitzt er die Passwörter sämtlicher Accounts. Das möchte man also vermeiden

Eine Möglichkeit, dem zu begegnen, ist es, die Passwörter zu *verschlüsseln*. Das Problem dabei ist aber, dass dann der Schlüssel dem Programm vorliegen muss. Ein Angreifer, der in den Besitz des Schlüssels gelangt, könnte dann die Passwörter entschlüsseln und man wäre so weit wie vorher.

Eine andere Möglichkeit besteht darin, in dieser Datei die Passwörter zu *hashen*. Statt des Passworts p wird also dessen Hash $H(p)$ gespeichert. Melde ich mich nun mit meinem Passwort p an, dann berechnet das System $H(p)$ und schaut, ob Benutzername und $H(p)$ in der Datei zusammen vorkommt.

Der Vorteil dieses Verfahrens liegt darin, dass es hier nichts zu entschlüsseln gibt. Da die verwendete Hashfunktion preimage resistant ist, kann man aus den gespeicherten Hashes die Passwörter nicht zurückberechnen. Produziert die Hashfunktion genügend lange Hashes, sollte auch Ausprobieren verschiedener Passwörter nichts nutzen: bei *n*-bit Hashes braucht es im Mittel 2^n Hashversuche, um ein preimage zu finden (siehe Punkt 2 oben). Damit könnte man die Passwortdatei auch veröffentlichen. (Frühe Versionen von Unix haben genau das gemacht.)

Das Problem besteht jedoch darin, dass die obige Argumentation nur funktioniert, *wenn alle möglichen Passwörter gleich wahrscheinlich sind*. Da aber Leute eher ein Passwort wie „passwort“ oder „123456“ wählen statt „7/jJKLLm;1“, ist das offensichtlich nicht der Fall. Gelangt man also in den Besitz eines gehashten Passworts *h*, kann man nach folgendem Plan vorgehen, um das preimage, also das Passwort, herauszufinden:

1. Lade von irgendwo eine Liste mit oft benutzen Passwörtern herunter.
2. Sortiere die Liste absteigend in der Reihenfolge ihrer Popularität. Das am häufigsten verwendete Passwort ist also das erste, das am wenigsten häufige das letzte Passwort in der Liste.
3. Führe Schritte 4 und 5 für alle Passwörter p nach der Beliebtheitsreihenfolge aus:
4. Berechne h’ = H(p).
5. Ist h = h’, gib p aus und beende den Lauf. Das Passwort ist geknackt. Ansonsten nimm das nächste Passwort p von der Liste und kehre zu Schritt 4 zurück.

Wenn das zu knackende Passwort ein häufig benutztes Passwort ist, führt dieser Ansatz weitaus schneller zum Ziel, als man das eigentlich erwarten sollte, wenn Passwörter alle gleich wahrscheinlich wären. Natürlich kann man diesen Algorithmus noch verfeinern, indem man das Passwort, das auf der Liste steht, noch leicht verändert, etwa durch Gross- und Kleinschreibung, oder durch das Anhängen von ein paar Ziffern. Damit wären dann auch Passwörter wie etwa *SupErMan99* abgedeckt.

Im Rest des Praktikums probieren Sie das nun aus.

Was Sie noch wissen müssen: Aus Gründen, die wir erst in der Vorlesung *Data Integrity and Authentication* besprechen können, wird in der Passwortdatei nicht einfach der zu einem Passwort *p* gehörende Hash gespeichert. Stattdessen wird für jeden Benutzer ein anderer, zufälliger, Wert *s* bestimmt, der *salt*. Beim Hashen werden dann *s* und *p* aneinandergehängt. Gehasht wird also nicht *p*, sondern $s + p$. Gespeichert werden dann der Benutzername, der Salt *s* und der Hash $h = H(s + p)$. Bei der Anmeldung wird das Passwort *p* vom Benutzer übermittelt. Das System schaut dann den Salt *s* und den Hash *h* in der Passwortdatei nach, berechnet $H(s + p)$ und schaut, ob das mit dem gespeicherten *h* übereinstimmt. Wenn ja, wird der Benutzer angemeldet, sonst nicht. Der Begriff *Salt* taucht an einigen Stellen im Praktikum auf, wird aber zur Beantwortung der Fragen nicht benötigt.

3 Einführung in John the Ripper[1]

John the Ripper (oder kurz *john*) ist ein Open Source Password-Cracking Tool. Das Tool kann auf verschiedenen Plattformen verwendet werden und ist auf dem Kali Linux-Image bereits installiert.

john wird in einem Terminal wie folgt verwendet:

```
$ john [options] password_file
```

password_file ist die Datei, welche die Passwörter beinhaltet, die Sie knacken wollen. Dies können z.B. Passwort-Hashes sein. Die möglichen Optionen, mit denen *john* gestartet werden kann, werden weiter unten bei den Beispielen erläutert.

john unterstützt vier verschiedene Modes, um Passwörter zu knacken:

Single Crack Mode

[1] https://www.openwall.com/john

Bei diesem Mode werden Kandidaten wie der Login Name oder der richtige Name des Benutzers (wenn vorhanden) als mögliche Passwortkandidaten getestet. Ebenfalls werden auf diese Kandidaten einige Mangling-Rules angewandt (z.B. Variieren der Gross-/Kleinschreibung oder Anhängen einer Ziffer), um weitere Varianten zu testen.

Wordlist Mode

Für diesen Mode müssen Sie eine Wörterliste (auch Dictionary genannt) spezifizieren, die verschiedene «likely passwords» enthält (also Passwörter, die häufig benutzt werden). Solche Wörterlisten finden Sie auch im Internet[2]. Optional kann zudem angegeben werden, dass *john* die in der Liste enthaltenen Passwörter nicht nur direkt verwenden soll, sondern auch Variationen davon (diese werden ebenfalls durch Mangling-Rules erzeugt).

Incremental Mode

Dieser Cracking-Mode entspricht einer Brute-Force Attacke. Es werden alle möglichen Zeichenkombinationen (Buchstaben, Ziffern, Sonderzeichen) durchprobiert. Dieser Mode dauert natürlich potentiell sehr lange. Wenn Sie allerdings eine kurze Passwortlänge oder einen kleinen Zeichensatz wählen, kann der Mode innerhalb nützlicher Frist enden.

External Mode

Diesen Mode werden Sie wahrscheinlich nicht verwenden. Der Vollständigkeit halber wird er hier aber trotzdem kurz erwähnt. Dieser Mode gibt Ihnen die Möglichkeit, einen eigenen Cracking-Mode zu definieren und diesen anzuwenden.

Beispiele

Im Folgenden sind ein paar Beispiele für den Gebrauch von *john* aufgelistet:

```
$ john password_file
```

Damit wird versucht, die Passwörter in der Datei *password_file* zu cracken. *john* verwendet dazu zuerst den Single Crack Mode, dann eine Wordlist (Default ist */usr/share/john/password.lst*, eine recht kleine Wörterliste mit 3'000 – 4'000 Einträgen) mit Mangling-Rules und schliesslich den Incremental Mode.

```
$ john --single password_file
$ john –-single password_file1 password_file2
```

Dies startet *john* im Single Crack Mode. Wie Sie sehen ist es auch möglich, mehrere Passwort-Files gleichzeitig zu verwenden.

```
$ john --wordlist=password.lst --rules password_file
```

Dies startet *john* im Wordlist Mode mit Mangling-Rules. Als Wordlist können Sie dabei irgendeine Wordlist-Datei verwenden.

```
$ john –-incremental[=mode] password_file
```

Dies startet *john* im Incremental Mode. Es gibt mehrere verschiedene Incremental Modes, z.B.:

- *all* – Komplettes US-ASCII Character Set (95 Zeichen); es werden alle damit möglichen Passwörter mit Länge 1 bis 8 Zeichen durchprobiert.
- *alpha* – 26 Zeichen (Kleinbuchstaben); Passwortlängen von 1 bis 8 Zeichen.
- *digits* – 10 Zeichen (Ziffern von 0-9); Passwortlängen von 1 bis 8 Zeichen.

[2] z.B. unter https://www.openwall.com/wordlists

- *alnum* – Kombiniert die Modes *alpha* und *digits*.

Der Default-Mode ist dabei all. Um *john* in einem bestimmten Incremental Mode zu starten, z.B. *alpha*, führen Sie folgendes aus:

```
$ john --incremental=alpha password_file
```

Ebenfalls kann ein Benutzer angegeben werden, wenn nur dessen Passwörter in *password_file* geknackt werden sollen:

```
$ john --incremental --users=user password_file
```

Dies startet *john* im Incremental Mode, es wird jedoch nur versucht, die Passwörter des Benutzers *user* zu cracken. Die Angabe von *--users* kann übrigens bei allen Modes verwendet werden.

Session wiederherstellen

john bietet die Möglichkeit, bestehende Cracking-Sessions zu unterbrechen, um sie zu einem späteren Zeitpunkt wieder fortzusetzen. Sessions können mit *Ctrl-C* unterbrochen werden. Sie können eine unterbrochene Session wie folgt fortsetzen:

```
$ john --restore password_file
```

Dabei ist *password_file* die Passwort-Datei, auf welcher Sie den Cracking-Vorgang fortsetzen wollen.

Geknackte Passwörter anschauen

john speichert geknackte Passwörter in der Datei *john.pot* ab (*~/.john/john.pot*). Um eine schöne Ausgabe aller bisher gecrackter Passwörter zu erhalten, geben Sie folgenden Befehl ein:

```
$ john --show password_file
```

password_file ist die Passwort-Datei, für welche die zugehörigen gecrackten Passwörter angezeigt werden sollen.

Status einer Session anschauen

Wenn Sie während einer laufenden Session die Enter-Taste drücken, zeigt *john* die Passwörter an, die gerade ausprobiert werden.

Konfigurationsdatei

Sämtliche Einstellungen (z.B. Mangling-Rules und die Modes für den Incremental Mode) sind in */etc/john/john.conf* konfiguriert und können angepasst werden.

4 Linux Password-Cracking mit *john*

Um erste Erfahrungen mit *john* zu sammeln werden Sie die Benutzerpasswörter des Kali Linux-Image knacken. Nehmen Sie an, ein Angreifer hat sich Zugang zum System verschafft und Zugriff auf die Passwort-Hashes erhalten und möchte diese nun offline knacken.

Die relevanten Dateien sind die folgenden:

- */etc/passwd* beinhaltet die Benutzernamen mit (wenn spezifiziert) zusätzlichen Informationen wie z.B. Vor- und Nachname.
- */etc/shadow* beinhaltet die Passwort-Hashes und die Salt-Werte. Je nach Linux-Version werden die Hashes unterschiedlich berechnet[3].

[3] Aktuell wird eine Hashfunktion namens SHA-512 verwendet, um aus Passwort und Salt-Wert den Hash zu berechnen. Diese Hashfunktion liefert einen Hash von 512 bit Länge und wird ausserdem noch 5000 mal iteriert.

Als erstes müssen die beiden Dateien zusammengefügt werden. Führen Sie dies gleich aus. Dies geschieht mit dem untenstehenden Befehl (in einem Terminal). Da */etc/shadow* nur von *root* lesbar ist, müssen Sie zusätzlich den *sudo* Befehl verwenden (und das Passwort *kali* eingeben):

```
$ sudo unshadow /etc/passwd /etc/shadow > linux_password_hashes
```

linux_password_hashes beinhaltet nun die zusammengefügten Dateien. Schauen Sie die erzeugte Datei kurz an, sie enthält insbesondere die Benutzernamen, die Salt-Werte, die Passwort-Hashes und Vor- und Nachname wenn vorhanden. Anschliessend können Sie *john* starten:

```
$ john linux_password_hashes
```

Bereits nach kurzer Zeit wird *john* einige Passwörter gefunden haben. Beim Drücken der Enter-Taste meldet *john* jeweils, welche Passwörter gerade ausprobiert werden. Dabei sieht man auch den aktuellen Mode: 1/3 für Single Crack Mode, 2/3 für Wordlist Mode und 3/3 für Incremental Mode. Ebenfalls wird angegeben, wieviele % des aktuellen Modes bereits abgearbeitet wurden und wann der Mode voraussichtlich beendet sein wird (ETA). Wird ein Passwort gefunden, dann wird die ETA typischerweise reduziert, da ja nun ein Passwort-Hash weniger getestet werden muss. Ebenfalls wird ausgegeben, wieviele Passwörter pro Sekunde getestet werden (*c/s*). Lassen Sie *john* eine gewisse Zeit laufen (mind. sieben Passwörter sollten Sie finden, das kann 20 Minuten dauern), Sie können ja bereits mit den weiteren Aufgaben weitermachen.

Insgesamt gibt es acht Benutzer. Geben Sie in der folgenden Tabelle an, welche Passwörter *john* gefunden hat. Geben Sie ebenfalls den jeweiligen Mode an, mit welchem Ihrer Meinung das Passwort gefunden wurde. Zur Erinnerung: Die verwendete Wordlist ist */usr/share/john/password.lst*.

Username	**Passwort**	**Wie von *john* gefunden?**
andy	Hugentobler5	single crack
eddie	Garfield	word list
james	pinkfloyd9	word list
kali	kali	single crack
root	root	single crack
snoopy	015168	incremental
superman		
thomas	samantha	word list

5 Authentisierung mit NTLM

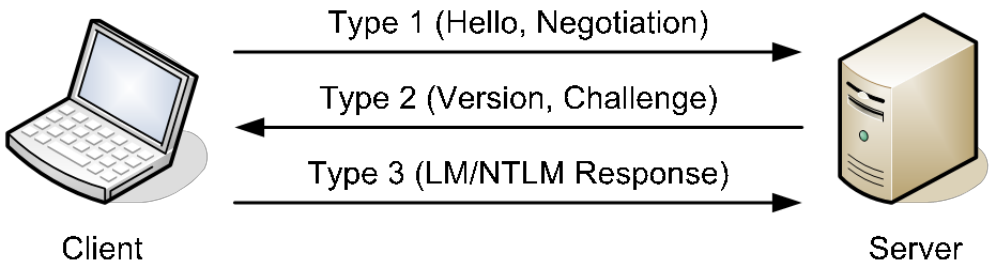
Den Rest des Praktikums widmen Sie dem NTLM-Protokoll (NT LAN Manager) und wie man dabei verwendete Passwörter knacken kann. NTLM wird in der Vorlesung in einem späteren Kapitel noch detaillierter eingeführt. NTLM basiert auf dem früheren Protokoll LM (LAN Manager) und wurde von Microsoft entwickelt. NTLM war vor Windows 2000 das primäre Authentisierungsverfahren in Windows-Domänen. Seither übernimmt diese Rolle Kerberos, allerdings wird NTLM auch in den modernsten Windows-Versionen (und auch auf anderen Systemen) aus Gründen der Rückwärtskompatibilität nach wie vor unterstützt und auch oft eingesetzt. In Nicht-Domänen-Umgebungen wird für die Peer-to-Peer Authentisierung (direkter Zugriff eines Windows-Rechners auf einen anderen) immer NTLM verwendet. Der häufigste Anwendungsfall in diesem Zusammenhang ist das File/Directory

---

Ist also p das Passwort, speichert Linux $H(H(H(\ldots H(\text{p})\ldots)))$ ab, wobei hier 5000 mal H = SHA-512 aufgerufen wird.

Sharing, das auf den Protokollen SMB (Server Message Block) bzw. CIFS (Common Internet File System) basiert.

NTLM gibt's in verschiedenen Versionen und alle sind immer noch im Einsatz: die erste Version NTLMv1 und die zweite Version NTLMv2. Daneben gibt es noch eine Version mit dem Namen NTLM Session Security (manchmal auch als NTLMv2 Session Security bezeichnet). Der Ablauf der Authentisierung ist prinzipiell in allen Versionen (inklusive dem Vorgänger LM) derselbe. Das Protokoll ist ein Challenge-Response Verfahren und ist nachfolgend dargestellt:



Damit sich der Client beim Server authentisieren kann, registriert sich der Client zunächst beim Server mit einem gehashten Passwort.

Wenn ein Client auf einen Server zugreifen möchte (z.B. um auf einen File-Share zuzugreifen), so initiiert der Client den Authentisierungsvorgang gemäss obiger Abbildung. Dazu schickt er zuerst eine sogenannte Type 1 Nachricht an den Server. Diese sagt im wesentlichen «Hallo, ich möchte Deinen Dienst nutzen. Ich benutze NTML Version *V*».

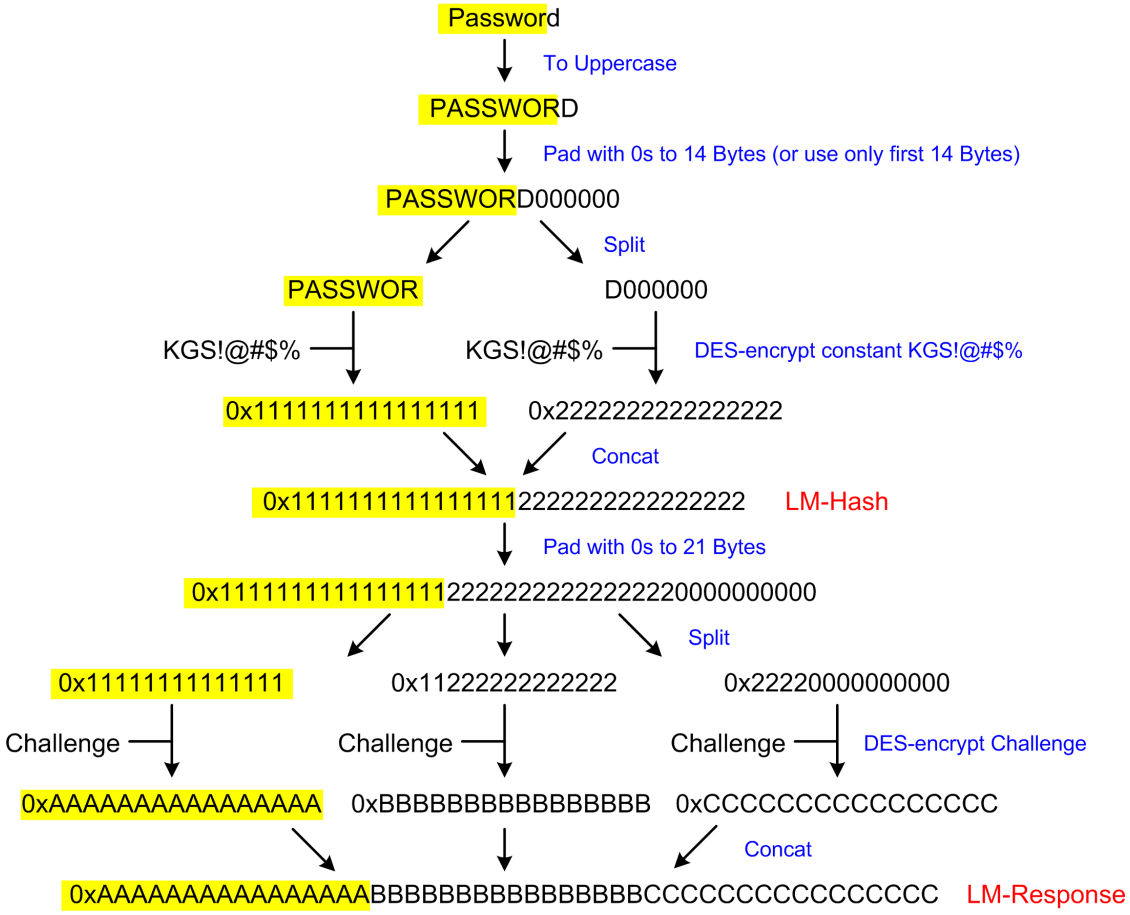
Ein Server antwortet auf die Anfrage mit einer Type 2 Meldung. Diese enthält neben der vom Server unterstützen Version *V'* auch eine *challenge*, in diesem Fall einen zufälligen Bitstring.

Um sich zu authentifizieren, verwendet der Client sein gehashtes Passwort als Schlüssel, um die Challenge zu verschlüsseln. Diese verschlüsselte Challenge schickt er als *Response* an den Server zurück. Sie haben noch keine Verschlüsselungsalgorithmen kennengelernt. Für dieses Praktikum ist es nur wichtig, dass Sie wissen, dass man ohne Kenntnis des Schlüssels (also des gehashten Passworts) die richtige Response zu einer gegebenen Challenge nicht berechnen kann.

Auf dieses Verfahren kann man nun eine Attacke durchführen, die im Prinzip mit jedem Passwort-basierten Challenge-Response Protokoll funktioniert. Man snifft den ganzen Authentisierungsvorgang und erhält dadurch die verwendete Version, die Challenge und die Response. Nun lassen sich in bekannter Manier Dictionary- und Brute-Force-Attacken darauf ausführen, indem ein Passwort gewählt wird, der resultierende LM- oder NT-Hash berechnet wird und die Response basierend auf der Challenge berechnet wird. Entspricht die berechnete Response der gesnifften Response, so hat man das Passwort gefunden. Falls man als Angreifer die Challenge im Voraus kennt oder diesen selbst wählen kann, kann man zudem für alle möglichen Passwörter (zumindest bis zu einer gewissen Passwortkomplexität, je nach verfügbarer Rechenpower) die resultierenden Responses vorausberechnen und sogenannte Rainbow Tables verwenden. Mehr zu diesen Rainbow Tables folgt später. Im Allgemeinen gilt natürlich, dass die Attacken umso aufwändiger werden, je komplexer das herauszufindende Passwort ist.

Berechnung der LM-Response

LM weist eine grundlegende Schwachstelle auf, die wir später ausnutzen wollen. Sie liegt einerseits in der Berechnung des LM-Hash aus dem Passwort und andererseits der Berechnung der LM-Response aus der Challenge und dem LM-Hash. Der Ablauf ist in der nachfolgenden Abbildung dargestellt und zeigt, wie aus einem Passwort *Password* zuerst der LM-Hash und dann damit basierend auf der Challenge des Servers die LM-Response berechnet wird. (Lassen Sie sich nicht davon irritieren, dass hier von «DES-Verschlüsselung» gesprochen wird. Sie müssen hier nichts über Verschlüsselung wissen. Wenn Sie das aber umtreibt, behandeln Sie hier «DES-Verschlüsselung» einfach wie einen weiteren Kasten, ähnlich wie eine Hashfunktion: Gleiche Eingaben geben gleiche Ausgaben, verschiedene Eingaben geben zufällige Ausgaben.)



Dabei sind insbesondere zwei Dinge auffällig: Zum einen wird für die Berechnung des LM-Hash das Passwort in Grossbuchstaben umgewandelt, wodurch jedes Passwort signifikant an Stärke verliert (Passwörter dürfen auch Ziffern und Sonderzeichen erhalten, die von dieser Umwandlung in Grossbuchstaben nicht betroffen sind). Zum anderen führen die ersten sieben Zeichen des Passworts direkt zum ersten Drittel der LM-Response ohne dass dies von den weiteren Zeichen des Passworts beeinflusst wird; siehe dazu die gelb unterlegten Zeichen in der obigen Abbildung. Dies heisst, dass diese sieben Zeichen später komplett separat geknackt werden können. Da ein Passwort höchstens 14 Zeichen beinhalten kann (allfällig weitere Zeichen werden beim Bilden des LM-Hash einfach ignoriert), muss im zweiten Schritt dann nochmals ein Passwort mit sieben Zeichen geknackt werden. Das unabhängige Knacken von zwei Passwörtern mit sieben Zeichen ist natürlich sehr viel einfacher als alle 14 Zeichen gemeinsam zu knacken.

Berechnung der NTLMv1-Response

NTLMv1 macht die Sache nicht viel besser, aber immerhin werden im ersten Schritt die Kleinbuchstaben im Passwort *nicht* in Grossbuchstaben umgewandelt. Zuerst wird ein MD4-Hash über dem Passwort berechnet, was in einem 128-bit langen Wert resultiert. Diese 16 Bytes werden mit 5 Null-Bytes auf 21 Bytes verlängert, woraus drei Gruppen mit je 7 Bytes generiert werden. Diese drei 7-byte Werte werden dann wie bei LM oben dargestellt verwendet, um die Challenge dreimal mit DES zu verschlüsseln.

Ein Angreifer, der Challenge und zugehörige Response abfängt, muss daher «nur» zwei DES-Verschlüsselungen knacken, um die ersten 14 Bytes des MD4-Hashes zu erhalten. Das Knacken der dritten DES-Verschlüsselung ist trivial, weil alle Bytes ausser den ersten beiden Null-Bytes sind. Der Angreifer erhält damit zwar nur den MD4-Hash und nicht das dahinterliegende Passwort, aber der

MD4-Hash reicht dem Angreifer, um sich im Namen des Benutzers mit NTLMv1 zu authentisieren[4]. Das Knacken eines DES-Schlüssels ist natürlich nach wie vor nicht ganz trivial, in Abschnitt 9 werden Sie aber noch erfahren, dass dies auch für Privatpersonen gegen Bezahlung problemlos machbar ist.

Berechnung der NTLMv2-Response

NTLMv2 (und auch NTLM Session Security) weist die Schwachstellen von LM und NTLMv1 nicht auf. Ein weiterer Vorteil ist, dass auch der Client eine Challenge für die Berechnung der Response beisteuert (es ist bei Sicherheitsprotokollen immer eine gute Idee, wenn beide Parteien Zufallsdaten beisteuern, damit z.B. ein Angreifer, der sich als Server ausgibt, nicht einfach alle beigesteuerten Zufallsdaten selbst wählen kann). Ein schlecht gewähltes Passwort ist aber natürlich trotzdem einfach knackbar.

In den nächsten Abschnitten werden Sie nun verschiedene Passwort-Cracking Methoden auf NTLM anwenden.

6 NTLM Attacke Teil 1: Dictionary Attacke auf NTLMv2

Es gibt mehrere Möglichkeiten, wie ein Angreifer an die NTLM-Challenges und -Responses gelangen kann, z.B.:

- Als Man-in-the-Middle (MITM) die Kommunikation zwischen Client und Server sniffen, wodurch die komplette Authentisierung und insbesondere die Challenges und zugehörigen Responses erhalten werden. MITM kann man – wie Sie in einem anderen Praktikum gelernt haben oder noch lernen werden – sehr einfach mittels ARP Spoofing (z.B. mit dem Tool Ettercap) werden. Leider gibt Ettercap die relevanten Authentisierungsdaten (Challenges & Responses) nicht aus, wodurch man diese selbst aus den aufgezeichneten Daten extrahieren muss.
- Man gibt sich als Server aus und bringt einen Benutzer dazu, einen Anmeldevorgang durchzuführen. Dazu könnte man beispielsweise dem Benutzer eine E-Mail senden mit einem \\SERVER\SHARE Link. Je nach E-Mail Client wird automatisch oder nach einem Klick des Benutzers auf den Link eine Verbindung aufgebaut und damit eine Authentisierung durchgeführt.

Weil Ettercap wie gesagt die erste Variante nicht komfortabel unterstützt und damit Sie noch ein weiteres Tool kennenlernen, verwenden wir hier die zweite Variante.

Für den Server verwenden wir das *Metasploit Framework*[5]. Metasploit ist ein sehr mächtiges Framework zum Ausnutzen diverser Schwachstellen. In unserem Fall wird Metasploit einen Samba-Server simulieren, bei welchem sich Benutzer mit NTLM authentisieren sollen.

Starten Sie in einem Terminal die Metasploit Framework Console – *msfconsole* (das dauert ein bisschen), die *root*-Rechte benötigt:

```
$ sudo msfconsole
```

Simulieren Sie dann einen Samba-Server, um Responses zu sammeln, indem Sie innerhalb von *msfconsole* folgendes eingeben:

```
use auxiliary/server/capture/smb
```

Als nächstes spezifizieren Sie, dass die verwendeten Challenges & Responses in Dateien mit dem Präfix *john* auf dem Desktop abgespeichert werden:

```
set JOHNPWFILE /home/kali/Desktop/john
```

[4] https://www.microsoft.com/security/blog/2012/12/11/new-guidance-to-mitigate-determined-adversaries-favorite-attack-pass-the-hash/

[5] https://www.metasploit.com

Diese Dateien können dann von *john* verwendet werden, um die Passwörter zu knacken.

Mit

```
info
```

können Sie die aktuellen Settings anzeigen. Interessant ist dabei die Challenge *1122334455667788*. Der Metasploit Samba-Server sendet standardmässig immer diese Challenge an den Client. Dies wird weiter unten bei der Verwendung von Rainbow Tables relevant sein.

Mit

```
run
```

wird der Server gestartet und mit

```
netstat -ntlp
```

können Sie prüfen, dass der Server wirklich auf TCP Port 445 horcht.

Benutzerseitig verwenden wir *smbclient* als Samba-Client. Melden Sie sich (am besten in einem anderen Terminal-Fenster) als *user4* mit Password *springfield* beim Server an:

```
$ smbclient //localhost/share -U user4
```

Die Anmeldung wird fehlschlagen, da es dem Metasploit Samba-Server ja nur darum geht, die Responses zu erhalten. Zudem existiert Benutzer *user4* (und auch die im Folgenden verwendeten Benutzer) auf dem System gar nicht.

Die *msfconsole* sollte einen Output der folgenden Art liefern:

```
[*] SMB Captured - 2022-01-15 09:25:30 +0100
NTLMv2 Response Captured from 127.0.0.1:59395 - 127.0.0.1
USER:user4 DOMAIN:WORKGROUP OS:Unix LM:Samba
LMHASH:Disabled
LM_CLIENT_CHALLENGE:Disabled
NTHASH:958fa99bc0f7eae891a2612e38f790cc
NT_CLIENT_CHALLENGE:0101000000000000f9d159cb11cf01fd0bb74bb300
e30c000000000200120057004f0052004b00470052004f005500500000000000
```

Was erkennt man hier:

- Es wird NTLMv2 verwendet – also die sichere NTLM-Variante. *smbclient* ist also standardmässig so konfiguriert, dass NTLMv2 verwendet wird.
- Die Challenge des Clients und die zugehörige Response. Bei NTLMv2 wird die 16 Byte lange Response (im Output oben mit NTHASH bezeichnet) mittels HMAC-MD5 über einer 8 Byte langen Challenge des Servers (diese ist im Output oben nicht ersichtlich) und einer 8 Byte langen Challenge des Clients (diese ist oben in NT_CLIENT_CHALLENGE enthalten) berechnet.

Auf dem Desktop sollte zudem ein File aufgetaucht sein, *john_netntlmv2*. Dieses beinhaltet den Benutzernamen, die verwendeten Challenges und die zugehörige Response in einem Format, so dass die Files von *john* verarbeitet werden können:

```
user4::WORKGROUP:1122334455667788:958fa99bc0f7eae891a2612e38f79
0cc:0101000000000000f9d159cb11cf01fd0bb74bb300e30c00000000020
0120057004f0052004b00470052004f005500500000000000
```

Am Anfang (nach *WORKGROUP:*) steht dabei die Challenge des Servers, für die – wie bereits weiter oben erwähnt – der Metasploit Samba-Server standardmässig immer *1122334455667788* verwendet.

Verwenden Sie nun *john*, um das Passwort zu knacken. Wechseln Sie dazu im Terminal am besten in das *Desktop* Verzeichnis (*/home/kali/Desktop*), damit Sie direkt auf die von *msfconsole* erzeugten Files zugreifen können. Als Wordlist verwenden Sie eine längere Liste als die Default-Wordlist, sie enthält rund 88'000 Einträge:

```
/usr/share/wordlists/metasploit/password.lst
```

Wie lautet der Aufruf von *john* (verwenden Sie nur den Wordlist Mode, siehe Abschnitt 2) und wie lange dauert es, bis *john* das Passwort gefunden hat? Hinweis: Sie müssen zuvor die evtl. noch laufende *john* Cracking-Session aus Abschnitt 4 beenden.

john --wordlist=/usr/share/wordlists/metasploit/password.lst --rules ./john_netntlmv2

Zeitdauer =~ 1s

john kann also auch NTLMv2-Responses knacken und Sie sehen auch, dass die Attacke in diesem Fall sehr effizient ist. Für jedes Passwort aus der Wörterliste hat *john* basierend auf den Challenges von Client und Server die NTLMv2-Response berechnet und mit dem erwarteten Wert verglichen. Stimmen die Werte überein, ist das Passwort gefunden. Man beachte auch, dass die Rate der getesteten Passwörter nun viel höher als bei den Linux Systempasswörtern ist und sie sollte «einige 1'000'000» betragen. Dies hat damit zu tun, dass nun pro getestet Passwort nur ein MD4-Hash und eine HMAC-MD5 Operation durchgeführt werden muss, was sehr effizient gemacht werden kann.

Machen Sie einen weiteren Versuch mit *user5* und *springfield5* als Passwort. Wie lautet der Aufruf von *john* und wie lange dauert es, bis *john* das Passwort gefunden hat? Wenn das Passwort nicht gefunden wird, dann haben Sie vermutlich eine Option vergessen, siehe Abschnitt 2.

john --wordlist=/usr/share/wordlists/metasploit/password.lst --rules ./john_netntlmv2

Zeitdauer =~ 1s

Auch dieses Passwort wurde also sehr schnell gefunden. Verwenden Sie nun *user6* und *springfield55* und versuchen Sie erneut, dass Passwort gleich wie oben zu knacken. Was beobachten Sie? Wieso könnte dies so sein?

john kann das Passwort nicht herausfinden, da vielleicht die Regeln dies nicht zulassen.

Diese Limitierung können Sie umgehen, indem Sie die Mangling-Rules von *john* anpassen. Diese Rules verwenden eine sehr umfangreiche Syntax, Details finden Sie unter

```
https://www.openwall.com/john/doc/RULES.shtml
```

Die Regeln sind im Konfigurationsfile

```
/etc/john/john.conf
```

definiert und können beliebig adaptiert werden. Öffnen Sie die Datei (mit *sudo*) und suchen Sie die Wordlist-Rules (*[List.Rules:Wordlist]*). Ein paar Zeilen weiter finden Sie folgende Regel:

```
# Lowercase pure alphabetic words and append a digit or simple punctuation
<* >2 !?A l $[2!37954860.?]
```

Dies ist offensichtlich die Regel, mit welcher *springfield5* gefunden wurde. Die Regel versteht sich wie folgt:

- `<* >2`: Die Regel gilt für Wörter mit mehr als 2 Zeichen (`>2`); nach oben gibt es keine Grenze (`<*`).
- `!?A`: Die Regel soll nicht verwendet werden, wenn das Wort ein Zeichen der Klasse `?A` enthält. `?a` bezeichnet die Klasse aller Buchstaben (a-z, A-Z) und `?A` negiert diese Klasse (alle Zeichen ausser Buchstaben). Enthält das Wort also irgendwelche Zeichen, die nicht Buchstaben sind, so wird die Regel nicht verwendet.
- `l`: Wandelt das Wort in Kleinbuchstaben.
- `$[2!37954860.?]`: Hängt ein Zeichen aus der Liste an. Hier wird eine Regex-ähnliche Syntax verwendet, die eckigen Klammern bedeuten dabei «eines aus der Liste».

Fügen Sie nun eine Regel hinzu, die das Wort in Kleinbuchstaben wandelt und zwei Ziffern anhängt. Dies ist basierend auf der obigen Regel einfach:

```
# Lowercase pure alphabetic words and append two digits
<* >2 !?A l $[0-9] $[0-9]
```

Versuchen Sie nun erneut, das Passwort zu knacken. Was ist das Ergebnis?

```
john --wordlist=/usr/share/wordlists/metasploit/password.lst --rules ./john_netntlmv2

Zeitdauer = 10s
```

Beurteilen Sie kurz den Effekt dieser Änderung der Regeln. Wenn die Wörterliste 100'000 Einträge hat, wie viele zusätzliche Passworttests haben Sie mit dieser Konfigurationsänderung eingeführt? Was sollten Sie deshalb bei jeder Regel, die Sie hinzufügen, beachten?

```
Da nun jedes Wort aus der Liste noch zusätzlich 0-9 beinhalten kann:
10 * 100'000 = 1'000'000 Einträge
```

7 NTLM Attacke Teil 2: Brute-Force Attacke auf NTLMv2

Starten Sie eine weitere Authentisierung, diesmal mit *user7* und Passwort *kyxba*. Dieses Wort ist kaum in einer Wörterliste, also ist hier ein Brute-Force Attacke wohl erfolgreicher – dazu bietet *john* ja den Incremental Mode. Schauen wir zuerst wieder das Konfigurationsfile an.

Suchen Sie den Bereich mit den Incremental Modes *(# Incremental modes*). Etwas weiter unten finden Sie den Mode *[Incremental:Lower]*, damit werden alle möglichen Kombinationen von 1-13 Klein-

buchstaben getestet – was vermutlich zu lange dauern würde, um in nützlicher Zeit ans Ziel zu gelangen (*lower.chr* bezeichnet den Zeichensatz bestehend aus Kleinbuchstaben).

Fügen Sie deshalb einen eigenen Mode hinzu, um Passwörter mit *1-5 Kleinbuchstaben* zu testen. Die Konfiguration sieht wie folgt aus, sie sollte selbsterklärend sein:

```
[Incremental:Lower15]
File = $JOHN/lower.chr
MinLen = 1
MaxLen = 5
CharCount = 26
```

Basierend auf dem *c/s* Wert auf Ihrem System, wie lange wird es ungefähr dauern, alle Passwörter zu testen?

k = 26^5 = 11'881'376 Kombinationen
Passwörter pro Sekunde = 5'362'000c/s

k / (c/s) =~ 2.22s

Führen Sie die Attacke durch. Verwenden Sie bei *john* die Option

```
--incremental=Lower15
```

Konnten Sie das Passwort finden? Stimmt die Suchdauer mit der obigen Abschätzung überein?

john --incremental=Lower15 ./john_netntlmv2

Zeitdauer =~ 1s

Längere Passwörter oder das Verwenden eines grösseren Charsets wird die Brute-Force Attacke schnell ans Limit bringen. Betrachten wir als nächstes ein Passwort, dass statt nur 5 Kleinbuchstaben ein 5-stelliges Passwort mit Klein- und Grossbuchstaben und Ziffern verwenden. Verwenden Sie dazu *user8* und Passwort *v7ZmP*. Wie viele mögliche Passwörter gibt es? Wie lange wird es in etwa dauern, alle Varianten durchzuprobieren? Betrachten Sie nur Passwörter der Länge 5 Zeichen:

k = (26*2+10)^5 = 916'132'832 Kombinationen
Passwörter pro Sekunde = 5'362'000c/s

k / (c/s) =~ 170.86s

Auch hier brauchen Sie einen Mode, der die entsprechenden Zeichen durchtestet. *john* bietet einen Mode *[Incremental:Alnum]*, die das Charset *alnum.chr* bestehend aus Kleinbuchstaben, Grossbuchstaben und Ziffern verwendet. Wie oben werden auch hier alle Kombinationen von 1-13 Zeichen getestet, was wiederum kaum in nützlicher Zeit zum Ziel führen würde. Auch hier kann man aber einen besser passenden Mode definieren, der Passwörter mit genau 5 Zeichen testet:

```
[Incremental:Alnum5]
File = $JOHN/alnum.chr
MinLen = 5
```

```
MaxLen = 5
CharCount = 62
```

Wir machen uns es hier aber noch etwas «komplizierter», damit Sie ein weiteres Feature des Incremental Mode kennenlernen. Nehmen Sie an, es gibt für den Fall kein passendes Charset, aber immerhin gibt es eines, das ein Subset der gewünschten Zeichen enthält. In diesem Fall können Sie mit der Option *Extra* weitere Zeichen hinzufügen.

Wir verwenden dies, um das Charset *lowernum.chr*, das Kleinbuchstaben und Ziffern beinhaltet, mit Grossbuchstaben zu ergänzen:

```
[Incremental:Alnum5]
File = $JOHN/lowernum.chr
Extra = ABCDEFGHIJKLMNOPQRSTUVWXYZ
MinLen = 5
MaxLen = 5
CharCount = 62
```

Fügen Sie diesen Mode hinzu und knacken Sie das Passwort. Lassen Sie *john* rechnen und fahren Sie mit dem Praktikum weiter. Wie lange hat es effektiv gedauert? Stimmt das mit Ihrer Erwartung überein?

```
john --incremental=Alnum5 ./john_netntlmv2

Zeitdauer = 2min 31s
Erwartet =~ 170.86s -> 2min 51s
```

Das ist natürlich immer noch überhaupt nicht sicher, aber immerhin etwas besser als die 5 Kleinbuchstaben. Jedes zusätzliche Zeichen erhöht die Passwortstärke enorm: Bei 6 Zeichen (Klein- und Grossbuchstaben und Ziffern) sind wir bei 57 Milliarden Kombinationen, was auf einem State-of-the-Art PC etwa 6 Stunden benötigt. 7 Zeichen entsprechen 3.5 Billionen Kombinationen oder rund 15 Tage und ab 8 Zeichen nähern wir uns so langsam dem Bereich, wo der benötigte Rechenaufwand für «Privatpersonen» doch langsam sehr aufwändig wird (220 Billionen Kombinationen und ca. 2.5 Jahre). Denken Sie aber auch daran, dass man die Brute-Force Attacke (wie jede «Passwort-Ausprobier-Attacke») perfekt auf mehrere Rechner verteilen kann und gewisse Institutionen (NSA etc.) vermutlich über enorme Rechenpower verfügen (bei 1'000 PCs dauert es dann nur noch rund einen Tag statt 2.5 Jahre). Zudem kann man günstige Rechenpower in der Cloud nutzen (siehe Abschnitt 9) oder auch spezielle Hardware anschaffen, um die Testrate massiv zu erhöhen. Für wirklich sensitive und wertvolle Daten, die einem Angreifer den Einsatz von «einigen PC-Jahren» Wert sind, sind 8 zufällig gewählte Zeichen also definitiv immer noch nicht sicher genug.

Als Fazit dieser Dictionary und Brute-Force Attacken können Sie folgendes mitnehmen: Auch wenn das verwendete Protokoll als sicher betrachtet wird, was bei dem hier verwendeten NTLMv2 grundsätzlich der Fall ist, so kann die Sicherheit durch schlecht gewählte Passwörter völlig kompromittiert weden.

8 NTLM Attacke Teil 3: Aktive Man-in-the-Middle Attacke mit Version-Downgrading und Cryptanalysis mit Rainbow Tables

Im letzten Teil arbeiten Sie mit *user9* und Passwort *n3PuLX76Ce*. Das Passwort enthält 10 Zeichen bestehend aus Klein- und Grossbuchstaben und Ziffern und die einzelnen Zeichen sind zufällig gewählt, wodurch Dictionary Attacken ziemlich aussichtslos sind. Wie sieht's mit einer Brute-Force Attacke aus? Die vorgegebenen Zeichen erlauben rund $8.4 \cdot 10^{17}$ mögliche Passwortkombinationen der Länge 10 Zeichen, was einer Bitstärke von etwa 60 Bits entspricht und damit schon «ordentlich si-

cher» ist. Ein aktueller Rechner braucht dafür etwa 10'000 Jahre. Vergessen wir also auch die lokale Brute-Force Attacke...

Dennoch gibt es eine sehr praktikable Attacke auf dieses Passwort. Was wir hier ausnutzen wollen ist die oben beschriebene Schwachstelle von LM. Dazu muss man den Client aber natürlich dazu bringen, LM zu verwenden. Dies kann man mit einer Version Downgrading Attacke machen. Der Angreifer agiert dabei als MITM und manipuliert in der ersten Phase der Authentisierung die Message vom Server zum Client so, dass der Client meint, der Server unterstützt nur das alte LM-Protokoll. Wenn der Client so konfiguriert ist, dass er das LM-Protokoll ebenfalls unterstützt, dann wird er sich mittels LM authentisieren. Ettercap enthält ein entsprechendes Downgrading Plugin, um dies durchzuführen.

Eine andere Variante ist die Verwendung des Metasploit Samba-Servers. Wenn der Client diesem ankündigt, dass er LM unterstützt, dann wird der Server den Client auffordern, sich mit LM zu authentisieren – der Server führt das Version-Downgrading also gleich selbst durch.

Welche Systeme unterstützen heute noch LM? Sämtliche modernen Systeme sollten heute so konfiguriert sein, dass sie per Default kein LM mehr verwenden. Seitens Microsoft war Windows XP z.B. die letzte Version, die LM standardmässig noch aktiviert hatte – dort funktioniert die Attacke also auf jeden Fall. Aber auch die neuesten Windows-Systeme können so konfiguriert werden, dass LM immer noch unterstützt wird – was in einer Firma, in der noch ältere Services verwendet werden die kein NTLMv2 unterstützen, durchaus der Fall sein kann.

Auch aktuelle Linux Versionen verwenden per Default kein LM mehr, man kann es aber aktivieren. Editieren Sie dazu die Samba Konfigurationsdatei

```
/etc/samba/smb.conf
```

und fügen Sie zu Beginn bei den *[global]* Settings die Zeilen

```
client lanman auth = yes
client ntlmv2 auth = no
```

hinzu. Authentisieren Sie sich dann mit smbclient unter Verwendung von *user9* mit Passwort *n3PuLX76Ce*. Die *msfconsole* sollte einen Output der folgenden Art liefern:

```
[*] SMB Captured - 2022-01-15 13:48:24 +0100
NTLMv1 Response Captured from 127.0.0.1:58147 - 127.0.0.1
USER:user9 DOMAIN:WORKGROUP OS:Unix LM:Samba
LMHASH:4b7826ecf3233eb7b80f4cd71576ed5ee1b26ea80ce2ee54
NTHASH:3cbbb19ac9c11aeb454f134578f2c5397e99a620fd9614c3
```

Wie Sie sehen wird jetzt NTLMv1 verwendet und es werden die LM-Response und die NTLMv1-Response mitgesendet.

Auf dem Desktop sollte zudem ein weiteres File *john_netntlm* aufgetaucht sein. Dieses enthält den Benutzernamen, die Challenge des Servers und die beiden Responses:

```
user9::WORKGROUP:4b7826ecf3233eb7b80f4cd71576ed5ee1b26ea80ce2ee
54:3cbbb19ac9c11aeb454f134578f2c5397e99a620fd9614c3:11223344556
67788
```

Das Format des Hex-Strings ist LM-Response:NTLMv1-Response:Challenge.

Wie Sie in Abschnitt 5 gelernt haben, werden LM zuerst alle Kleinbuchstaben im Passwort in Grossbuchstaben umwandeln, was in N3PULX76CE resultiert. Das sind plötzlich nur noch 36 mögliche Varianten für jedes Zeichen des Passworts, was insgesamt nur noch rund $3.65 \cdot 10^{15}$ Passwortkombinationen ergibt und einer Bitstärke von etwa 52 Bits entspricht. Eine Brute-Force Attacke auf das gan-

ze Passwort ist damit schon mal etwa 230 mal einfacher geworden, trivial ist das aber immer noch nicht.

Zusätzlich nutzen wir die Tatsache aus, dass wir bei LM die ersten Zeichen des Passworts unabhängig vom Rest knacken können. Die ersten 7 Zeichen entsprechen N3PULX7 und es gibt «nur» etwa 80 Milliarden mögliche Passwortkombinationen dieser Art. Dies können Sie mit *john* mit einer Brute-Force Attacke auf einem aktuellen Rechner in wenigen Stunden knacken. *john* bietet dafür einen speziellen Cracking-Mode, den Sie mit der Option *--format=nethalflm* aktivieren. Zudem müssen Sie einen passenden Incremental Mode angeben. Im vorliegenden Fall eignet sich *UpperNum*, weil das dabei verwendete Charset Grossbuchstaben und Ziffern beinhaltet. Der zu verwendende Befehl wäre damit wie folgt:

```
john --format=nethalflm --incremental=UpperNum password_file
```

Das dauert uns aber immer noch etwas zu lang. Um diese Zeit weiter zu verkürzen, verwenden Sie Cryptanalysis mit Rainbow Tables.

Die Idee ist, dass man alle möglichen LM-Responses vorausberechnet. Man nimmt also die 80 Milliarden Passwörter (wir nehmen an, der Angreifer weiss, dass nur Buchstaben und Ziffern verwendet werden) und berechnet die 80 Milliarden resultierenden LM-Responses und speichert dies als Tabelle. Man muss dann nur noch die abgefangene LM-Response in der Tabelle suchen und man erhält direkt die ersten sieben Zeichen des Passworts, ohne dass man nochmals LM-Responses berechnen müsste. Jetzt sehen Sie auch, warum der Server immer die Challenge *1122334455667788* verwendet: Für die Vorausberechnung der Tabelle müssen Sie die Challenge wissen (diese fliesst ja in die Berechnung der LM-Responses mit ein). Das Berechnen dieser 80 Milliarden LM-Responses ist keine sehr aufwendige Sache, man kann dies auf einem modernen PC in weniger als einem Tag durchführen und man muss dies (für einen gegebenen Challenge) nur einmal machen und kann die Tabelle dann in jeder Attacke wiederverwenden. Das Problem ist der Speicherplatz, um die Tabelle abzuspeichern: Ein Passwort braucht 12 Bytes, eine LM-Response ist 24 Bytes lang, macht 36 Bytes pro Eintrag. Bei 80 Milliarden Einträgen macht dies 2.88 Terabytes. Das ist zwar durchführbar, Sie brauchen aber doch einiges an Disk-Space dafür. Schön wäre es, wenn man das Ganze in einer kompakteren Form abspeichern könnte. Dazu dienen die Rainbow Tables.

Rainbow Tables ist im Wesentlichen eine Datenstruktur, die 2003 von Philippe Oechslin (EPFL) publiziert wurde[6]. Wir gehen hier nicht auf die Details ein, was genau dahintersteckt; eine sehr anschauliche Erklärung ist hier[7] zu finden. Die Grundidee der Erstellung einer Rainbow Table ist die folgende: Ein zufälliges Passwort wird gewählt (aus dem Bereich der in Frage kommenden Passwörter; in unserem Fall also Passwörter mit einer Länge von sieben Zeichen bestehend aus Grossbuchstaben und Ziffern) und der daraus gehashte oder verschlüsselte Wert berechnet. In unserem Fall ist das die LM-Response, das Prinzip ist aber für beliebige Verfahren anwendbar, wo basierend auf einem Passwort «irgendetwas» verschlüsselt oder gehasht wird. Der Einfachheit nehmen wir im Folgenden an, dass ein Passwort auf einen Hash abgebildet wird. Nachdem also im ersten Schritt ein zufällig gewähltes Passwort auf den Hash abgebildet wird, wird im nächsten Schritt aus diesem Hash wird mit Hilfe einer Formel wieder ein Passwort berechnet, von welchem wiederum der Hashwert erzeugt wird. Von diesem Hash wird dann wieder ein Passwort erzeugt, und so weiter. Nach einer bestimmten (einstellbaren) Anzahl von Durchläufen wird alles gelöscht, außer dem Anfang und dem Ende der Kette (erstes Passwort und letzter Hash). Danach werden in gleicher Manier weitere Ketten erstellt, wobei jeweils ein neues, zufälliges Startpasswort gewählt wird. Um basierend auf dieser Rainbow Table das zu einem Hash passende Passwort zu finden, wird zuerst die Kette gesucht, in der das Passwort sein muss. Dies verlangt das wiederum Berechnen von Hashes (maximal so viele, wie eine Kette lang ist). Hat man die Kette gefunden, ergibt sich daraus direkt das gesuchte Passwort, indem man sich ausgehenden vom ersten Passwort nochmals durch die gefundene Kette durchrechnet, bis der berechnete Hash dem

[6] https://lasecwww.epfl.ch/pub/lasec/doc/Oech03.pdf

[7] http://kestas.kuliukas.com/RainbowTables/

gesuchten Hash entspricht. Das unmittelbar davor gefundene Passwort ist dann das gesuchte Passwort. Den gewonnenen Speicherplatz erkaufen Sie sich also mit einer erhöhten Rechenzeit, um ein Passwort zu finden. Nebenbei: Wenn Sie das Verfahren wirklich verstehen wollen, so kommen Sie nicht darum herum, den angegebenen Link mit der anschaulichen Erklärung zu studieren.

Es existieren verschiedene Programme, um Rainbow Tables zu erzeugen, z.B. RainbowCrack[8]. Ebenfalls werden Rainbow Tabes im Internet gehandelt (oder auch gratis[9] angeboten), wo man sich im Wesentlichen den Rechenaufwand, um die Rainbow Tables zu erstellen, erkauft. Zudem gibt es Online-Services, die selbst grosse Rainbow Tables besitzen und denen Sie einen Hash senden können, worauf das passende Passwort für Sie gefunden wird.

Für das vorliegende Problem (Passwörter mit sieben Grossbuchstaben und Ziffern) kann man auf einem aktuellen PC in etwa einem halben Tag eine Rainbow Table erzeugen, die 40 Millionen Ketten mit einer Kettenlänge von 2'500 enthält. Damit finden Sie aus einer LM-Response mit 60%-iger Wahrscheinlichkeit das Passwort (Rainbow Tables sind probabilistisch, auch darauf wollen wir hier nicht detailliert eingehen). Mit drei solchen Tabellen (Rechenaufwand von gut 1½ Tagen) erreicht man eine Erfolgswahrscheinlichkeit von 94%. Jede dieser Tabellen hat eine Grösse von 610 MB, wir brauchen gesamthaft für die drei Tabellen also einen Speicherplatz von knapp 2 GB, was rund 1'500 mal weniger als die komplette Tabelle von Passwörtern und LM-Responses ist. Drei solche Tabellen wurden mit dem Tool WinRTGen[10] vorausberechnet und stehen Ihnen unter */home/kali/rainbowtables* zu Verfügung.

Jetzt sind Sie bereit, das 10-stellige Passwort zu knacken. Dazu verwenden wir ein weiteres Tool, *rcracki_mt*. Rufen Sie es wie folgt auf:

```
$ rcracki_mt -h 4b7826ecf3233eb7 /home/kali/rainbowtables/halflmchall*
```

Für die Option *-h* müssen Sie dabei die ersten 8 Bytes der LM-Response aus *john_netntlm* verwenden, dies entspricht *4b7826ecf3233eb7*. Der Stern am Schluss ist notwendig, damit alle drei Rainbow Tables verwendet werden. Was meldet das Tool und wie lange dauert die Suche?

```
plaintext found:                1 of 1(100.00%)
total disk access time:         15.73s
total cryptanalysis time:       0.21s
total pre-calculation time:     1.62s
total chain walk step:          3121251
total false alarm:              209
total chain walk step due to false alarm: 393523

result
--------------------------------------------------
4b7826ecf3233eb7    N3PULX7 hex:4e3350554c5837
```

Es fehlen noch die restlichen drei Zeichen des Passworts. Diese knacken Sie mit einer Brute-Force Attacke mit Hilfe des Tools *netntlm.pl*[11] (befindet sich im Verzeichnis */usr/local/bin*). Dieses Tool verwendet *john* und nimmt selbstständig die notwendigen Konfigurationen vor, um den zweiten Teil eines LM-Response zu knacken. Als Parameter werden die ersten 7 Zeichen des Passworts (*--seed*) und die Datei *john_netntlm* benötigt:

```
$ netntlm.pl --seed N3PULX7 --file john_netntlm
```

Was ist das Ergebnis uns wie lange dauert die Analyse?

[8] http://project-rainbowcrack.com

[9] https://www.freerainbowtables.com

[10] http://www.oxid.it/projects.html

[11] https://github.com/piyushcse29/john-the-ripper/blob/master/run/netntlm.pl

Kombination gefunden
Zeitdauer 2s

Jetzt geht es nur noch darum, das richtige Passwort (mit Klein- und Grossbuchstaben) zu finden. Dies ist grundsätzlich sehr einfach, denn man muss einfach bei den Buchstaben im Passwort alle Klein/Grossbuchstaben-Varianten durchprobieren. Mit der NTLMv1-Response, die ja auch bei der Authentisierung mitgesendet wurde, kann man dies einfach prüfen. netntlm.pl kann auch dies durchführen, indem derselbe Befehl wie oben ohne `--seed` Parameter verwendet wird:

```
$ netntlm.pl --file john_netntlm
```

Was ist hier das Ergebnis? Wie lange dauerte diese Analyse?

Password gefunden
Zeitdauer <1s

Zusammenfassend haben wir folgendes erreicht: Wir haben ein Passwort der Stärke 60 Bits, für welches wir eigentlich etwa 10'000 Jahre benötigt hätten, in wenigen Sekunden reiner Rechenzeit geknackt. Dabei haben wir ausgenutzt, dass man das NTLM-Protokoll als Angreifer einfach downgraden kann und dann eine Schwachstelle im LM-Authentisierungsverfahren ausgenutzt. Nicht schlecht… (OK, wir haben die Berechnung der Rainbow Tables nicht eingerechnet, aber das muss man ja nur einmal und nicht «einmal pro Attacke» tun.)

9 Password-Cracking – Schlussbemerkungen

Sie haben gesehen, dass es heute mächtige Tools für das Offline Password-Cracking gibt. Sind Passwörter schlecht gewählt (Wörter aus einem Dictionary, allenfalls leicht verändert), dann ist es oft sehr einfach, diese in kurzer Zeit zu knacken. Auch kurze zufällige Passwörter sind schnell herausgefunden, auch wenn hier der Aufwand mit zunehmender Passwortlänge exponentiell ansteigt.

Bei komplexeren Passwörtern können Ihnen – wie Sie ebenfalls gesehen haben –Rainbow Tables helfen. Wenn Sie jetzt denken, Rainbow Tables sind enorm toll und damit kann man alles sehr schnell knacken, so müssen Sie sich daran erinnern, dass Rainbow Tables einfach den Vorteil der Kompaktheit haben. Das Berechnen der Rainbow Tables ist genau so aufwändig, wie wenn Sie eine «normale» komplette Passwort-Hash Tabelle erstellen. Wenn Sie z.B. Passwörter bis 8 Zeichen annehmen, die als Zeichen Klein- und Grossbuchstaben, Ziffern und 14 Sonderzeichen zulassen und eine Rainbow Table für die MD5-Hashes dieser Passwörter berechnen wollen, die mit 60%-iger Wahrscheinlichkeit ein Passwort findet, dann brauchen Sie eine Table mit 4 Milliarden Ketten der Länge 250'000. Die Berechnung auf einem aktuellen Rechner dauert dafür rund 16 Jahre. Dafür ist der benötigte Speicherplatz nur etwa 60 GB, während eine komplette Tabelle aller Passwörter und Hashes 500'000 mal so viel Platz benötigt.

Wichtig ist auch zu realisieren, dass das Vorberechnen von irgendwelchen Tabellen nur dann hilft, wenn der Angreifer auch alle Werte (ausser dem Passwort) kennt, die in die Berechnung einfliessen. Deshalb ist es bei Protokollen immer eine gute Idee, wenn beide Seiten Zufallswerte bzw. eine Challenge einfliessen lassen. Dies ist z.B. bei NTLMv2 der Fall: Der Angreifer kann zwar immer noch die Challenge vom Server spoofen, der Client wählt aber einen weiteren Challenge für die Response-Berechnung und der Angreifer weiss diesen natürlich nicht im Voraus. Aus dem gleichen Grund wird Salt beim Abspeichern von gehashten Passwörtern auf einem System verwendet: dadurch werden

Precompiled Dictionary Attacks unterbunden, denn der Angreifer kann keine passende Tabelle von wahrscheinlichen Passwörtern und zugehörigen Hashes im Voraus berechnen (bevor die Passwortdatei mit den Salt-Werten und den Hashes erhält).

Ein jüngerer Trend beim Password-Cracking ist das Ausnutzen der Rechenkapazitäten in der Cloud. Der Service CloudCracker[12], der heute nicht mehr existiert, bot Password-Cracking gegen Bezahlung an. Man konnte z.B. einen NTLMv1-Hash (oder auch einen MS-CHAPv2-Hash, das ist das identische Protokoll) an den Service senden, um den zugehörigen MD4-Hash zu erhalten. Gemäss Erklärungen in Abschnitt 5 verwendet NTLMv1 wie LM auch DES mit je einer Hälfte des MD4-Hashes, macht aber immerhin den Fehler nicht, Klein- in Grossbuchstaben zu konvertieren. Und da aus dem Passwort zuerst ein MD4-Hash berechnet wird, werden auch nicht nur die druckbaren Zeichen, sondern beliebige Bytes verwendet. Man muss also eine Brute-Force Attacke durchführen, um den MD4-Hash zu finden. DES verwendet einen 56-bit Schlüssel, das sind $2^{56} = 72 \cdot 10^{15}$ mögliche Schlüssel. Um beide Hälften des MD4-Hashes zu knacken, müssen als $144 \cdot 10^{15}$ Schlüssel durchprobiert werden. Auf einem lokalen Rechner oder auch auf ein paar lokalen Rechnern ist dies nicht praktikabel. CloudCracker führte dies in 21 Stunden für USD 100 durch (Stand Januar 2014). DES ist also definitiv nicht mehr sicher...

Die NTLM Downgrading Attacke sollte heute in den meisten Fällen nicht mehr möglich sein, da nur noch wenige Systeme im Einsatz sind, die LM per Default unterstützen (unter anderem Windows XP). Sie zeigt aber ein wichtiges Grundproblem auf, wenn es von Protokollen ältere, verwundbare Versionen gibt: Es dauert auch beim Erscheinen der neuen Version dann oft sehr lange (viele Jahre), bis die älteren Versionen dann wirklich weg sind und es gibt meist eine lange Übergangsphase, in der die alte und neue Version unterstützt wird – damit neuere und ältere Geräte miteinander verwendet werden können. NTLM ist hier nur ein Beispiel. Ein anderes bekanntes Beispiel ist SSL/TLS, wo man bei der Version SSLv2 gravierende Mängel festgestellt hat (Mitte der 1990-er Jahre) und mit SSLv3 schnell Abhilfe geliefert hat (in der Zwischenzeit gilt allerdings auch SSLv3 als gebrochen), aber auch heute noch finden sich vereinzelte Clients und Server, die nach wie vor SSLv2 unterstützen.

Praktikumspunkte

In diesem Praktikum können Sie **2 Praktikumspunkte** erreichen. Laden Sie dazu die vier Files *alice_netntlmv2*, *bob_netntlmv2*, *carol_netntlm* und *dave_netntlm* von Moodle herunter (Sie finden die Files unter *password_hashes*). Die Files beinhalten Benutzernamen, Challenges und die zugehörigen LM-, NTLMv1- bzw. NTLMv2-Responses, so dass die Files von *john* verarbeitet werden können. Betrachten Sie in jedem der Files nur den für Ihre Gruppe relevanten Eintrag. Gruppe 13 arbeitet also mit den Benutzern *alice13*, *bob13*, *carol13* und *dave13*. Löschen Sie deshalb nach dem Download der Files sämtliche Zeilen, die *nicht* Ihre Benutzer betreffen.

Um die zwei Punkte zu erhalten müssen Sie die Passwörter der vier Benutzer, die Ihrer Gruppe entsprechen, knacken und per E-Mail an den Betreuer senden. Verwenden Sie *Security Lab - Password-Cracking - Gruppe X - Name1 Name2* als Subject; entsprechend Ihrer Gruppennummer und den Namen der Gruppenmitglieder. Ihre E-Mail muss für jedes der vier geknackten Passwörter folgendes enthalten:

- Das geknackte Passwort.
- Die Konfigurationsanpassung, die Sie an *john.conf* vorgenommen haben, um das Passwort zu knacken (falls dies notwendig war).
- Den Befehl oder die Befehle, den/die Sie verwendet haben, um das Passwort zu knacken (genauer Befehl, so wie Sie ihn im Terminal verwendet haben).

Um Ihnen das Knacken zu vereinfach gibt's ein paar Hinweise zu den Passwörtern:

- **alice (NTLMv2):** Das Passwort basiert auf einem Wort. Das letzte Zeichen des Worts ist ein Grossbuchstabe. Zusätzlich wurde vorne ein Sonderzeichen und am Ende eine Ziffer hinzugefügt.

[12] https://www.cloudcracker.com

Hinweis: `c` konvertiert das erste Zeichen in einen Grossbuchstaben und `r` dreht das Wort um. Evtl. können Sie damit eine *john*-Regel erzeugen, die das letzte Zeichen in einen Grossbuchstaben umwandeln? Zudem können Sie mit `^[...]` ein Zeichen aus einer Liste vorne hinzufügen.

- **bob (NTLMv2):** Das Passwort besteht aus 4 beliebigen druckbaren ASCII-Zeichen. Hinweis: Verwenden Sie das Charset *ascii.chr* als Basis.
- **carol (LM/NTLMv1):** Das Passwort besteht aus 11 Zeichen mit Kleinbuchstaben, Grossbuchstaben und Ziffern. Der zweite Teil des Crackens kann dabei (je nach Gruppe) recht lange dauern, allenfalls auch über eine Stunde. Lassen Sie in diesem Fall den Cracking-Vorgang einfach laufen und fahren Sie mit dem nächsten Passwort (*dave*) weiter.
- **dave (LM/NTLMv1):** Das Passwort besteht aus 10 Zeichen und verwendet die Hex-Zeichen `0-9`, `A-F` und die Sonderzeichen `+` und `/`.

```
alice:
[List.Rules:Alice]
<* >2 r c r ^[\!\,\;\:\-_\.\^\$\*\+\-\?\(\)\[\]\{\}\\\|\V] $[0-9]

john --wordlist=/usr/share/wordlists/metasploit/password.lst --rules=Alice ./alice_netntlmv2
->*dominiquE7      (alice14)


bob:
[Incremental:ASCII4]
File = $JOHN/ascii.chr
MinLen = 4
MaxLen = 4
CharCount = 95

john --incremental=ASCII4 ./bob_netntlmv2

jE6*            (bob14)


carol:
rcracki_mt -h f3c38a4d51f04223 /home/kali/rainbowtables/halflmchall*
-> f3c38a4d51f04223        5DMRWD6 hex:35444d52574436

netntlm.pl --seed 5DMRWD6 --file ./carol_netntlm
-> 5DMRWD6DMRE      (carol14)

netntlm.pl --file ./carol_netntlm
-> 5dmRWd6dMre      (carol14)


dave:
[Incremental:Digits10]
File = $JOHN/digits.chr
Extra = ABCDEF+/
MinLen = 7
MaxLen = 7
CharCount = 18

john --format=nethalflm --incremental=Digits10 ./dave_netntlm
-> 7/++FE2          (dave14)

netntlm.pl --seed 7/++FE2 --file ./dave_netntlm
-> 7/++FE2E8E       (dave14)
```