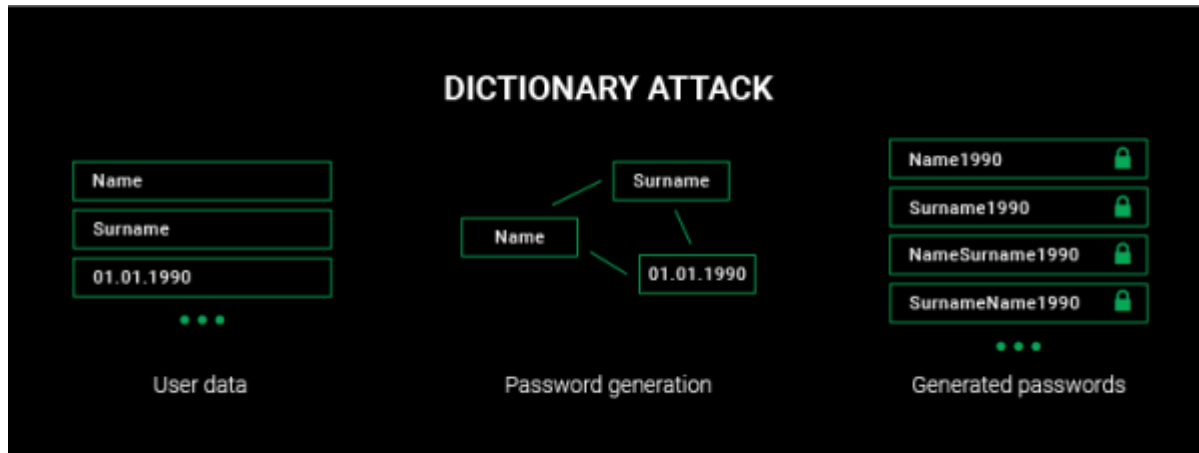


Dictionary / Wörterbuch

Anstatt zufällige Symbolkombinationen zu erraten, können Hacker auch vorhandene Wörter aus einem Wörterbuch durchprobieren. Oft verwenden Menschen Wörter in ihren Passwörtern, um sich diese besser merken zu können – das erleichtert Hackern die Arbeit. Brute-Force-Software kann sogar die Wörterbuchpasswörter mutieren, um die Erfolgschancen zu erhöhen.



Rainbow Tables

Rainbow tables sind vorberechnete Tabellen, die Hashwerte mit möglichen Klartextpasswörtern verknüpfen, um die inverse Suche zu beschleunigen. Statt jedes Passwort neu zu bruteforcen, schaut ein Angreifer den Hash nach in der Tabelle nach und findet so schnell das zugehörige Passwort, wenn vorhanden. Die Methode erfordert grosse Rechen- und Speicherressourcen fuer die Erstellung, reduziert aber die Kosten beim Angriff. Kurz gesagt: clever vorverarbeitetes Lookup.

RAINBOW TABLE

Plaintext	MD5 Checksum
123456	bfbKJ*(Y)BDnjin3219cbjwhc9HCNSdjin3210fhAJH*W*CnjwnkoIAFJC9N346
123456789	cbjwhc9HCNSdjin3210fhAJH*W*CnjwnkoIAFJC9N346NJRsd99x8andjnx932
password	ndcsanHN(UB*(Djnd3b293rgbfiJHD*hnfkajcc*HCnenfc3h82f9hcnAJnc982h3
12345678	jkbxnc198gbf9xm(M*A(MHD98mx3nfp9xpKjND*)DN@8Dnjq9ifnjeasc9q23v
qwerty	NJRsd99x8andmilkjn30q(&*XVBa8cbNBAkcbo98Oijknqc2h9*(BXJnnqfnjsic9
1234567	cn2390bcqijknsdzxcnu9b-cmwnoienvcv0*(&TGVXBxb87w*&XG8js9chscb\
111111	KNCSjEF*njemdzvndsnvi304bgsjNXB(SHCNUZnscknBAJNCisnfcna9*(&YBjk

From:
<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:
<https://wiki.bzz.ch/modul/m183/learningunits/lu09/02>

Last update: **2025/12/08 09:08**

