ANDREAS LÖNNHOLM – WEB SERVICES – INLÄMNING 2 – DEL 1

DICTIONARY ATTACK

En Dictionary attack är en brute-force-metodik som används för att bryta sig in i ett lösenordskyddat system genom att testa, ord för ord, i en lång lista gentemot en utvald dators lösenord i dess inloggningssystem. Metoden används även för att hitta nyckeln till krypterade eller hashade filer och system.

Själva ordlistan brukar innehålla alla vanliga ord, siffror, bokstäver och tecken.
Det är också vanligt att i ordlistan använda tidigare kända lösenord från stora attacker.

Ett exempel på listor från stora attacker är:
https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/

Detta gör att du blir extra sårbar om du återanvänder ditt lösenord på flera platser på Internet. Har du samma lösenord på tio olika sidor, och EN av dem på något vis läcker sin information är alla dina tio sidor ett lätt mål för den som utför en Dictionary attack.

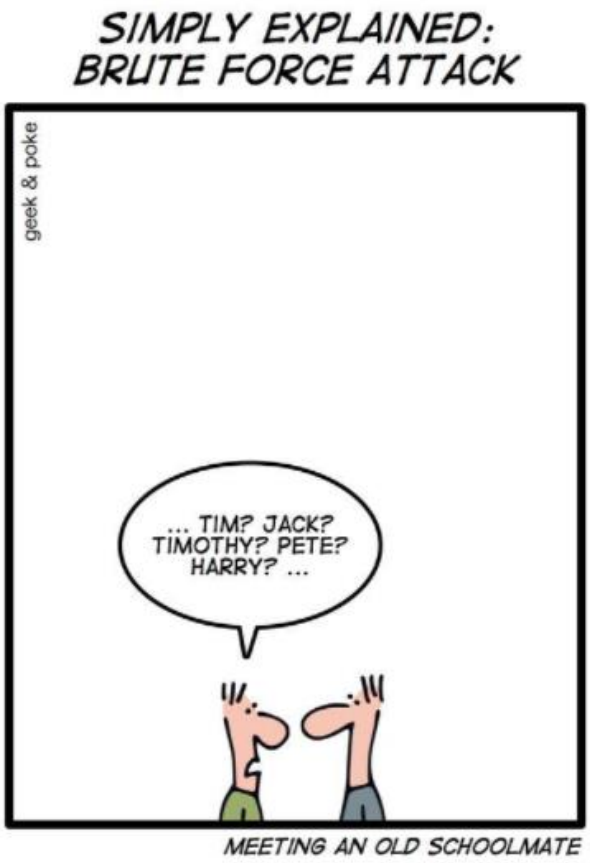
Vilka är lösningarna och vad löser de?

- Ett långt och komplext lösenord är ett effektivt försvar mot Brute-force-attacker av denna form. Gärna ett sådant så att du lätt kommer ihåg det också, i form av en längre mening där du exempelvis byter alla e mot siffran 3 eller O mot 0. Ett exempel är: ***!JagG1llarKanin3r!***

  Tänk på att aldrig ha ett lösenord som är logiskt. Det bör inte innehålla något relaterat till din återställningsfråga, ditt namn, ditt personnummer eller dina barn, din hustru och andra i din närhet. Detta är det första som används vid attacker.

  Ett ha ett långt lösenord som inte innehåller något som relaterat till dig som person kommer troligen inte att helt förhindra attacken, men kan göra att den tar så lång tid att den som utför den tröttnar eller ger sig på enklare mål i stället.

- Se till att lagra ditt lösenord på en säker plats, allra helst i en krypterad fil med hjälp av ett lösenordshanterarprogram.



Om tjänsten du använder lagrar information som är kritisk för dig, se då till att all kommunikation krypteras mellan dig och tjänsten.
Samt se över så att tjänsten i sig lagrar din data och ditt lösenord på ett säkert sätt.

Genom att lagra dina lösenord krypterade med ett lösenord för att kunna nå dem, hindrar du andra från att kolla över din axel för att se dem eller från att snabbt sätta sig vid din dator när du är borta. Även om detta inte heller blir helt säkert så har du skapat ett till lager som tar mer tid för den som vill få tag på din information, vilket gör dig till ett mindre intressant mål.

Samma sak gäller kryptering gentemot Internet-tjänster, där icke-krypterade källor innebär att du skickar allt i klartext, vilket lätt kan sniffas (avlyssnas med program).

Tyvärr är många vanliga krypteringstekniker rätt lättknäckta,
så ta ”säkerheten” kring dessa lösningar främst som en metod att fördröja attacker, inte som en total trygghet.

- Två-faktors-autensifiering. Där du till exempel behöver bekräfta med en kod som skickas som SMS till din mobil, för att kunna logga in i systemet.

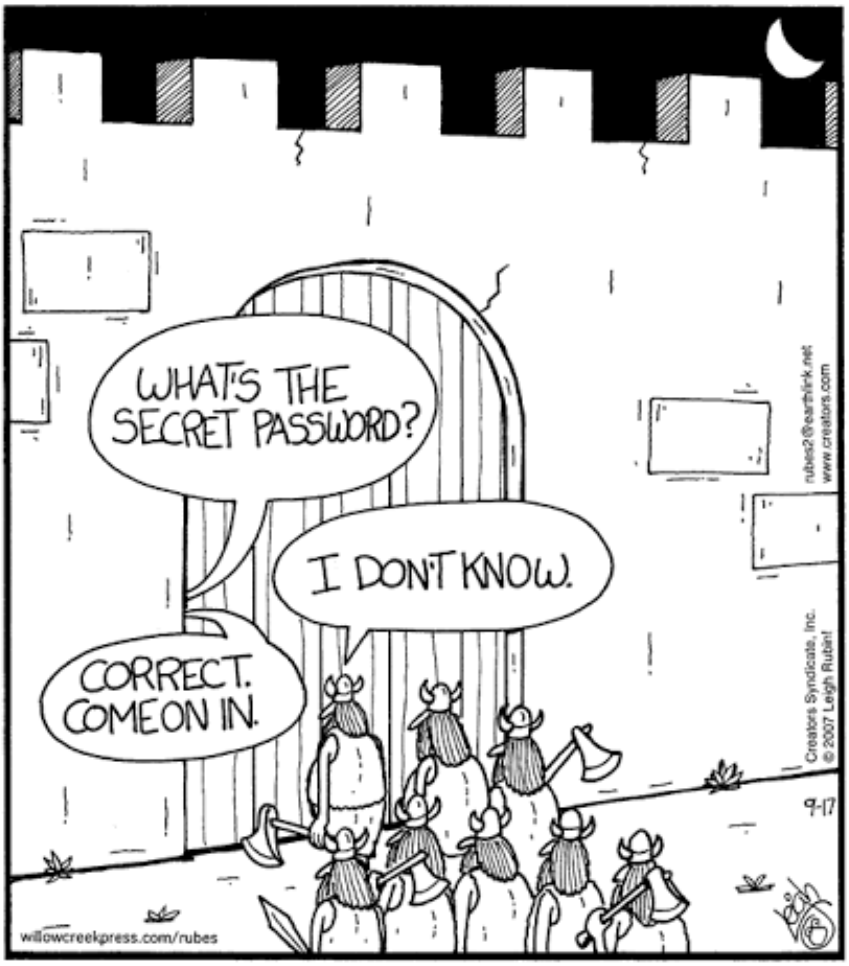
  Liknande upplägg kan även innebära att du måste ha ett fysiskt kort eller ett USB-minne istoppad i datorn för att få logga in.

  Detta är en mycket bra metod för att förhindra den här typen av attack.
  Även om en illvillig person kan komma över din USB-sticka eller mobil med hjälp av Social engineering (konsten att manipulera människor) så är det mindre troligt att du både läckt ditt lösenord och att denna person får tag på dina fysiska ägodelar.

- En annan lösning är att begränsa antalet inloggningsförsök per användare inom ett visst antal minuter, vilket även kan kombineras med att kontot låses helt efter ett visst antal försök, för att ytterligare öka säkerheten i system. Vanligt här är också att automatiskt skicka vidare till system-ansvarig när detta sker, så denna snabbt kan sätta in åtgärder.

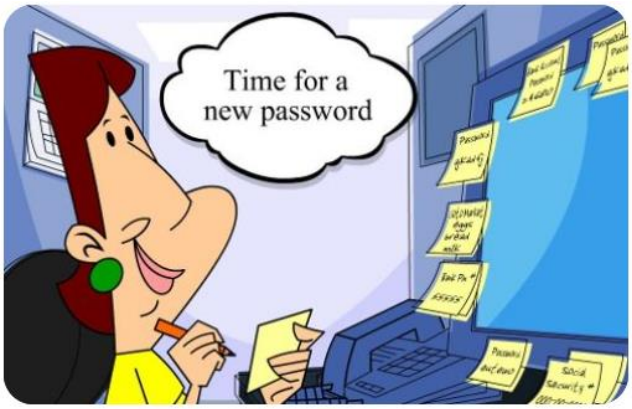
  Det sistnämnda är troligen det sätt som är allra bäst för att säkra sig gentemot denna typ av attack. För att på bara ett fåtal försök är det omöjligt att utföra en riktig Dictionary attack, då behöver den illvillige personen på något vis redan innan fått reda på hela eller stora delar av lösenordet.

  Notera dock att detta inte skyddar emot andra former av attacker, där den illvillige redan har fått tag på lösenordet.



Why great care and consideration should be taken when selecting the proper password

INTERN ATTACK



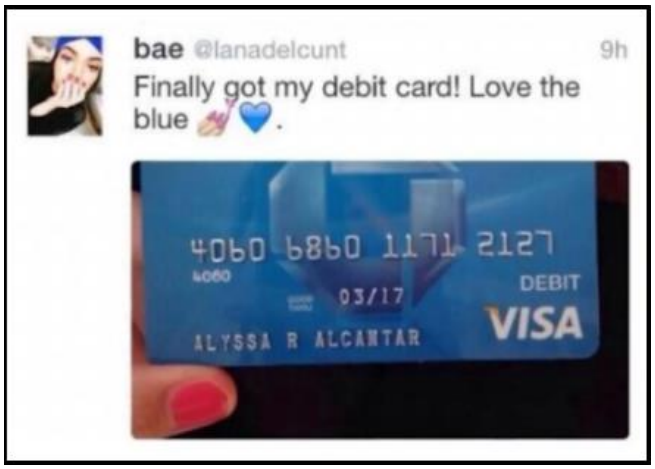
Internattacker är ett begrepp som innebär att någon inom organisation på något vis själv skapar en attack eller ger information till yttre part som möjliggör en attack.

Denna någon kan även vara yttre leverantörer, vars system är uppkopplade gentemot ditt företag, vilket kan resultera i att anställda på flera dussintals företag kan göra attacker mot din organisation.

Interna användare har ju rätten till att nå de interna systemen och dess information, vilket gör detta oerhört svårt att upptäcka för de som kontrollerar systemen.

Nedan nämns några exempel på olika interna attacker:

- Anställd som stjäl viktig kund-data och säljer detta vidare till yttre part
- Anställd som skriver sitt lösenord på en post-it-lapp väl synligt på skärmen
- Anställd som får trojan på sin dator och därmed ger tillgång till företagsmiljön till yttre part
- Anställd vars dator, med viktig information på, blir stulen
- Anställd som avslutat sin anställning där, medvetet förstör system eller viktig information för att han/hon inte velat få sparken
- Anställd som tar med information från gamla arbetsgivaren till den nya
- En vanlig mänsklig faktor är också att göra fel, som att skicka e-post till fel person eller förlägga viktiga saker, vilket kan utgöra ett säkerhetshot



Många, om inte alla dessa problem, relaterar till att vi är just människor.
Därför blir de svårlösta, då vår natur är så djupt rotad i oss. Vi förenklar saker för att komma ihåg (sätter post-It-lappar överallt) och vi tappar bort saker även om det är viktigt material. Dessutom råkar vi ibland skicka saker till fel person.

Det vi kan tänka på är att aldrig ge en anställd fler rättigheter till systemen än de absolut måste ha för att utföra sitt jobb. Om de då skulle, antingen medvetet eller omedvetet, råka ut för något så begränsas åtminstone skadan.

Precis som i Dictionary attack kan två-vägs-autensifiering eller en fysisk USB-sticka som krav för att logga in systemen hjälpa mot yttre anfall, ifall användaren råkat ge

bort sitt lösenord. Men detta hindrar ju inte om användaren både slarvat bort sitt lösenord och sin USB-sticka. Inte heller skyddar det om jobb-mobil eller -dator med allt innehåll som behövs för inloggning hamnat i fel händer.

Att ha bra rutiner kring hur man avslutar någons anställning är av stor vikt här. Omgående när någon slutat behöver personens konton spärras och alla ägodelar med viktigt företagsmaterial bör återföras till företaget.
Företaget bör därför ha listor över vad de har för utrustning och var viktiga saker finns. Detta för att åtminstone försöka begränsa illdåd, men även här finns ju den mänskliga faktorn så ingen perfekt lösning kommer troligen att finnas för denna typ av problem, någonsin.