10. Securitatea parolelor

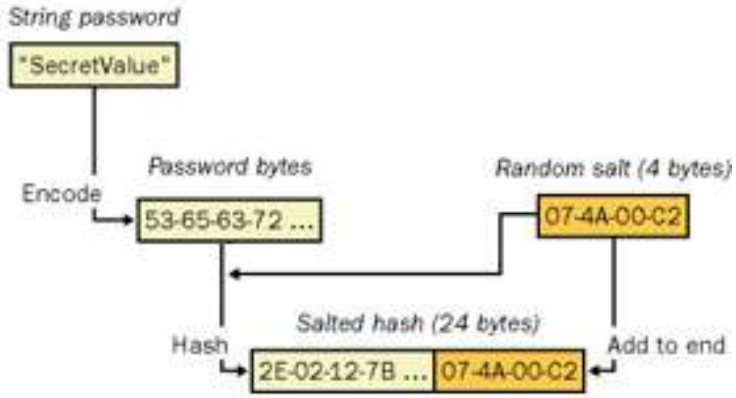
Securitatea parolelor

- Parola reprezintă cel mai folosit mecanism pentru autentificarea utilizatorilor la sisteme și aplicații
- Compromiterea unei parole are ca efect obținerea accesului în sistem
- Parolele sunt vulnerabile la o serie de atacuri
- Furtul identităţii reprezintă în momentul de faţă “infracţiunea informatică” cu cea mai mare rată de creştere

Reprezentarea parolelor

- De regula, parolele nu sunt stocate în clar pe sisteme ci codificat, sub formă de valori hash
  - folosirea de funcții one-way pentru codificare (DES, MD5, SHA, etc)
- Atunci când un utilizator introduce o parolă, se calculează valoarea hash și se compară cu valoarea stocată în baza de date
- Dacă cele două valori coincid, utilizatorul este autentificat

Reprezentarea parolelor (cont.)



- *Salting* – introducerea de date aleatoare în procesul de calcul al valorii hash
- Valoarea salt este stocată împreună cu valoarea hash în intrarea corespunzătoare utilizatorului
- Dacă doi utilizatori au parole identice, atunci acestea vor fi reprezentate diferit în baza de date
- Crește semnificativ nivelul de securitate – pentru fiecare parolă testată trebuie luate în considerare toate valorile posibile pentru salt

Tipuri de atacuri asupra parolelor

- Atacuri online
  - încercări repetate de logon
  - pot fi depistate relativ ușor
- Atacuri offline
  - obținerea parolelor din valorile hash stocate local sau transmise prin rețea
    - acces în sistem (cu drepturi administrative)
    - sniffing la nivel de rețea
  - nu pot fi depistate

Tipuri de atacuri asupra parolelor (cont.)

- De tip dicționar
  - se testează toate cuvintele dintr-un dicționar (fișier text)
  - rapidă (funcție de numărul de cuvinte din dicționar)
- Forța brută (brute force)
  - se testează toate combinațiile posibile de parole
  - necesită timp și putere de calcul
- Hibride
  - cuvinte din dicționar + combinații de numere și caractere speciale
  - Ex: *P@ssw0rd, password12, password$%*
- Rainbow tables
  - lookup tables
  - valori hash precalculate pentru un set dat de caractere și o lungime prestabilită a parolelor
  - necesită spațiu mare de stocare
- Keyloggers, phishing, social engineering

Windows passwords

- 2 tipuri diferite de valori hash
  - LM hash (LAN Manager hash)
    - folosite în protocolul de autentificare LAN Manager
    - Windows 95, 98, Me
  - NT hash (NTLM hash)
    - folosite în protocoalele de autentificare NTLMv1, NTLMv2 și Kerberos
- Valorile hash sunt stocate local în baza de date Security Accounts Manager (SAM) sau în Active Directory
- Baza de date SAM se află în directorul *Windows\system32\config*
  - Nu poate fi copiată cât timp sistemul este pornit (accesul este blocat de sistemul de operare)
  - Soluții:
    - se bootează de pe CD și se copiază fișierul (necesită acces fizic pe mașina țintă)
    - se folosește copia de rezervă din directorul: *Windows\repair.* Această copie se creează atunci când administratorul folosește utilitarul RDISK
- SYSKEY – criptare SAM

LM hash

- Calculul valorii hash:

```
Define LMOWFv1(Passwd, User, UserDom) as
       ConcatenationOf( DES( UpperCase( Passwd)[0..6],"KGS!@#$%"),
                        DES( UpperCase( Passwd)[7..13],"KGS!@#$%"))
EndDefine
```

- LM hash este relativ ușor de spart pentru parole scurte!
- Exemplu:
  - Fie parola: 123456abcdef
  - Se convertește la litere mari și se adaugă blank-uri până se obțin 14 caractere: 123456ABCDEF__
  - Se spage valoare rezultată în două părți și se criptează separat folosind algoritmul DES:
    123456A = 6BF11E04AFAB197F
    BCDEF__ = F1E9FFDCC75575B15
  - Valoarea hash corespunzătoare parolei date este:
    6BF11E04AFAB197FF1E9FFDCC75575B15
  - Folosind L0phtCrack, prima parte se poate sparge în aproximativ 24 ore iar cea de-a doua în 60 secunde
  - Dacă parola conține mai puțin de 7 caractere, atunci cea de-a doua parte a valori hash va fi aceiași:
    AAD3B435B51404EE

- NT 3.1 până la XP SP2 suportă LM hashes pentru asigurarea compatibilității cu versiunile mai vechi de sistem de operare și această funcționalitate este activată în mod implicit. Vista suportă însa funcționalitatea este dezactivată implicit.
  - se recomandă dezactivarea acestei opțiuni!

NT hash

- Suportă parole mai mari de 14 caractere
- Nu convertește parola la litere mari și nu o sparge în bucăți
- NTLMv1 (folosit până la Windows NT SP2)
  - calculul valorii hash:

```
Define NTOWFv1(Passwd, User, UserDom) as
  MD4(UNICODE(Passwd))
EndDefine
```

  - datorită unei slabiciuni, nu se recomandă folosirea lui!
- NTLMv2 (folosit începând cu Windows NT SP3)
  - calculul valorii hash:

```
Define NTOWFv2(Passwd, User, UserDom) as
  HMAC_MD5(MD4(UNICODE(Passwd)),
       ConcatenationOf(Uppercase(User),UserDom)
EndDefine
```

Extragerea hash-urilor din SAM

- **samdump2**
  - http://sourceforge.net/projects/ophcrack/files/
  - **Linux tool (BackTrack 4)**

```
#mount /dev/hda1 /mnt/XXX
#samdump2 /mnt/XXX/WINDOWS/system32/config/system
  /mnt/XXX/WINDOWS/system32/config/sam > hash.txt
```

- **pwdump(1-7)**
  - http://en.wikipedia.org/wiki/Pwdump
  - **Windows tool**

```
C:\>pwdump7 > hash.txt
```

- **fgdump**
  - http://swamp.foofus.net/fizzgig/fgdump/downloads.htm
  - **Windows tool**

```
C:\>fgdump -v
```

Extragerea hash-urilor din cache (registry)

- **Atunci când utilizatorul se loghează în domeniu, parola sa este stocată în registry pentru a putea fi folosită pentru logon offline**
- **creddump**
  - http://code.google.com/p/creddump/
  - Linux tool
- **cachedump**
  - ftp://ftp.openwall.com/john/contrib/cachedump/
  - Windows tool

Extragerea hash-urilor din rețea

- **fgdump**

```
C:\>fgdump -v -h hostname -u Username -p Password
```

- **pwdump6**

```
C:\>pwdump6 -u Username -p Password hostname
```

- **Ettercap**
  - http://ettercap.sourceforge.net/
- **Cain & Abel**
  - http://www.oxid.it/
- **L0phtCrack**
  - http://www.l0phtcrack.com/
- **KerbCrack**
  - http://www.ntsecurity.nu/toolbox/kerbcrack/
  - kerbsniff, kerbcrack
- **SMBRelay / SMBRelay2**
  - atacuri de tip MITM
  - http://www.xfocus.net/articles/200305/smbrelay.html

Spargerea parolelor Windows

- **John the Ripper**
  - http://www.openwall.com/john/
  - atacuri de tip brute-force, knownforce, dicţionar
  - Linux / Windows tool

```
#/usr/local/john/john hash.txt (LM hash)
#/usr/local/john/john --format:NT hash.txt (NT hash)
#/usr/local/john/john --format:mscash hash.txt (cached cred)
```

- **Cain & Abel**
  - http://www.oxid.it/
  - atacuri de tip brute-force, dicţionar, criptanaliză
- **L0phtCrack**
  - http://www.l0phtcrack.com/
  - atacuri de tip brute-force, dicţionar, hibride, rainbow tables
  - produs comercial

Spargerea parolelor Windows (cont.)

- **Ophcrack**
  - http://sourceforge.net/projects/ophcrack/files/
  - **NTLM rainbow tables trebuie cumpărate:**
    - http://www.objectif-securite.ch/en/products.php
  - **lungime 1 - 6:**
    0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUV WXYZ!"#$%&'()*+,-./:;&<=>?@[\]^_`{|}~ (space included)
  - **lungime 7:**
    0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUV WXYZ
  - **lungime 8:**
    0123456789abcdefghijklmnopqrstuvwxyz
- **RainbowCrack**
  - http://project-rainbowcrack.com/
  - **rainbow tables**

Resetarea parolelor

- Local Windows Password
  - ERD Commander
  - chntpw (BackTrack / System Rescue CD)
  - ntpassword (http://pogostick.net/~pnh/ntpasswd/)
- Active Directory Password
  - Resetting a windows 2003 domain account http://www.nobodix.org/seb/win2003_adminpass.html
  - Directory Restore Service Mode
  - SRVANY.EXED, INSTSRV.EXE (Resource Kit)

Unix passwords

- Parolele sunt stocate criptat în fișierul /etc/passwd (accesibil tuturor) sau /etc/shadow (accesibil numai root)
- Algoritmul de criptare DES în care textul de intrare este null iar cheia este parola utilizatorului
- Salt pe 12 biți – 4096 variante posibile pentru o parolă dată
- /etc/passwd

  username:passwd:UID:GID:full_name:directory:shell

  username:Npge08pfz4wuk:503:100:Full Name:/home/username:/bin/sh

  username:x:503:100:Full Name:/home/username:/bin/sh
- /etc/shadow

  username:passwd:last:may:must:warn:expire:disable:reserved

  username:Npge08pfz4wuk:9479:0:10000::::

Spargerea parolelor Unix

- **John the Ripper**

```
#unshadow /etc/passwd /etc/shadow >saltedpasswords
#john saltedpasswords
```

Atacuri online asupra parolelor

- **Hydra / XHydra**
  - http://freeworld.thc.org/thc-hydra/
  - grad ridicat de paralelism
  - Samba, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco
  - Suport pentru SSL

```
#hydra -l john -P passwords.txt -v 192.168.0.112 ftp
#hydra -l john -P passwords.txt -v 192.168.0.112 pop3
#hydra -P passwords.txt -v 192.168.0.112 snmp
```

- **Medusa**
  - http://www.foofus.net/
  - design modular, grad ridicat de paralelism
  - SMB, HTTP, POP3, MS-SQL, SSHv2, etc

```
#medusa -d
#medusa -h 192.168.0.100 -M ssh -U users.txt -P
  passwords.txt
```

Crearea de dicţionare proprii

- **CeWL (Custom Word List)**
  - http://www.digininja.org/projects/cewl.php

```
#cewl.rb -w wordlist.txt http://192.168.0.10
```

- **WYD**
  - http://www.remote-exploit.org/index.php/Wyd

```
#wyd.pl -o output.txt www.upb.ro
```

Parole default

- O serie de echipamente și aplicații, folosesc parole default în momentul instalării
- Parolele default trebuie schimbate cât mai repede posibil
- Phenolit List
  - http://www.phenoelit-us.org/dpl/dpl.html
- CIRT
  - 437 vendors, 1842 passwords
  - http://www.cirt.net/passwords

Metode de protecție

- Folosirea de parole complexe
- Schimbarea periodică a parolelor
- Blocarea conturilor după un număr de încercări nereușite de autentificare
  - Cum trebuie procedat cu contul de administrator ?
- Jurnalizarea încercărilor nereușite de autentificare