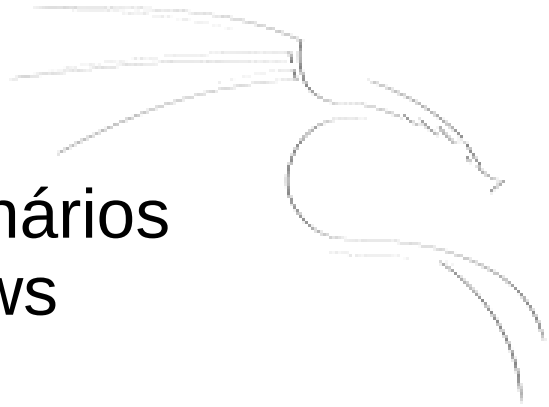
<password cracking>

EXPLAINED

Password Cracking

Agenda:

- Tipos de ataque,
- Hash,
- Wordlist,
- Rainbow Tables
- Criação de Dicionários
- Sistemas Windows
- Sistemas Linux
- HashCat
- Hydra
- John the Ripper
- OphCrack

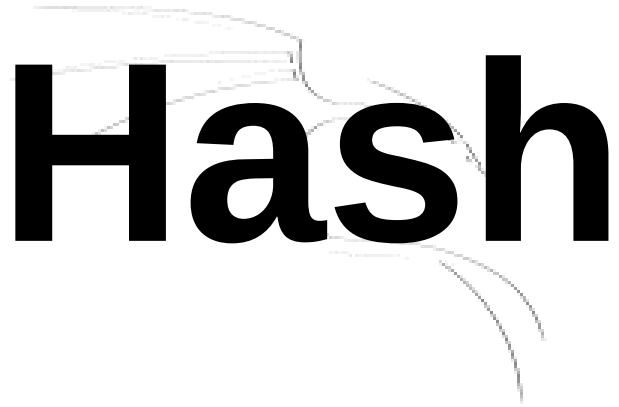


Password Cracking

Tipos de ataques:

- Ataques de Dicionário (guessing)
- Brute Force
- Rainbow Tables
- Social Engineering
- Malware

Password Cracking



Password Cracking

Características de uma função Hash:

- **Unidirecionalidade:** conhecido um resumo h(M), deve ser computacionalmente impossível encontrar M a partir do resumo.
- **Compressão:** a partir de uma mensagem de qualquer longitude, o resumo h(M) deve ter uma longitude fixa. O normal é que a longitude de h(M) seja menor do que a da mensagem M.
- **Facilidade de cálculo:** deve ser fácil calcular h(M) a partir de uma mensagem M.

Password Cracking

- **Difusão:** o resumo h(M) deve ser una função complexa de todos os bits da mensagem M: se, se modifica um só bit da mensagem M, o hash h(M) deveria mudar a metade dos seus bits aproximadamente.

- **Colisão:** será computacionalmente impossível, conhecido M, encontrar outro M' tal que h(M) = h(M'). Isto se conhece como resistência débil às colisões.

Exemplos de Algorítimos:
md4, md5, sha1, sha256, sha512

http://www.md5hashgenerator.com/
http://hash.online-convert.com/sha256-generator

Wordlist

Password Cracking

É um banco de dados de palavras que possuem as credenciais (usuário/senha ou somente a senha) de autenticação de um sistema. Quanto mais personalizado e biográfico para o alvo em questão é um wordlist (dicionário) maior será sua probabilidade obter o acesso ao sistema alvo.

Kali Linux:

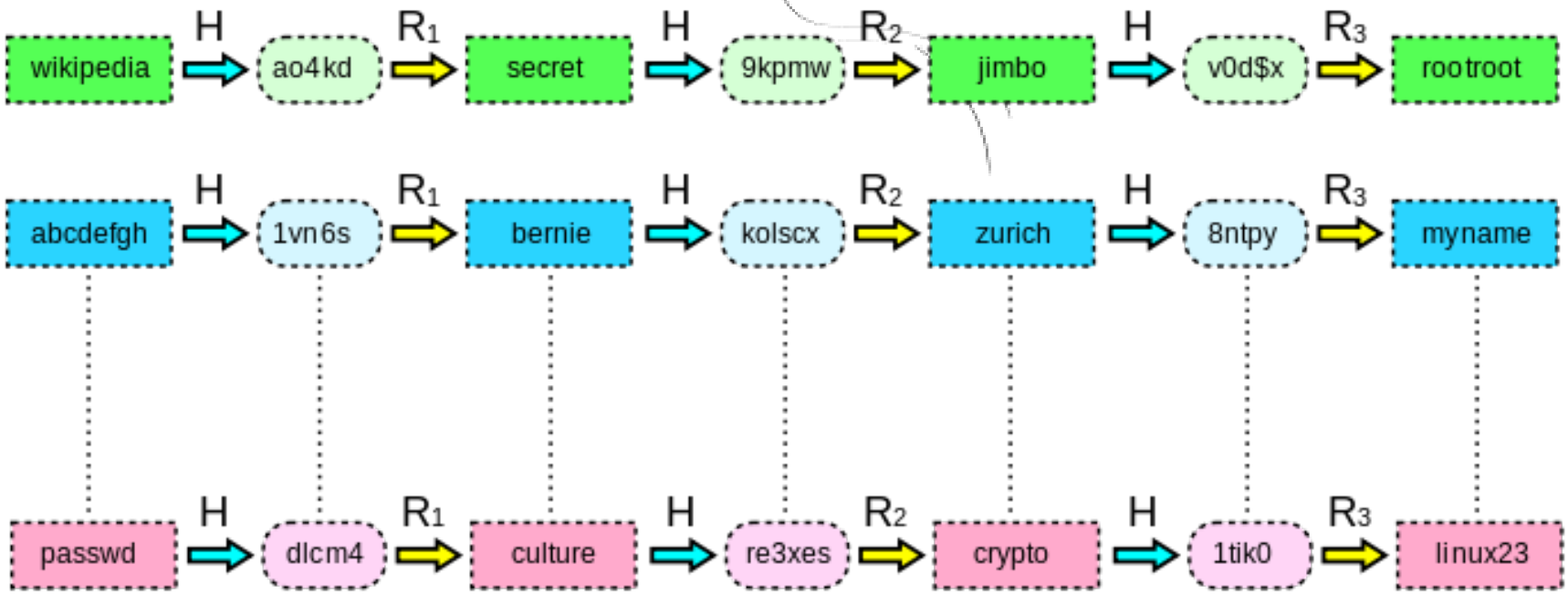
/usr/share/john/password.lst
/usr/share/wordlists/rockyou.txt

Rainbow Tables

Password Cracking

Tabela pré-computada utilizada para quebrar hashes de senhas.
As tabelas tem o intuito de economizar tempo/processamento da maquina em troca de espaço em disco.

http://ophcrack.sourceforge.net/tables.php



Make your own shit

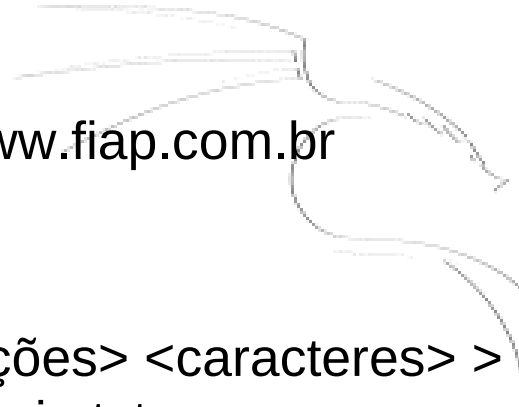
Password Cracking

CUPP

cupp -i

CeWL

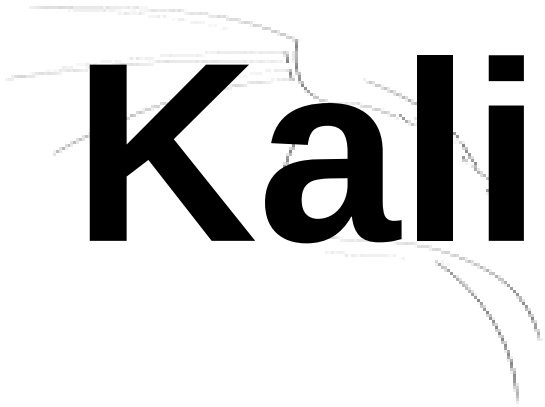
cewl <opções> URL
cewl -m5 -d2 -w fiap.txt www.fiap.com.br



CRUNCH

crunch <min> <max> <opções> <caracteres> > <arquivo>
crunch 5 5 admin > dicionario.txt
crunch 1 1 -p abcde > dicionario.txt
crunch 1 1 -p ab cd ef > dicionario.txt
crunch 9 9 -f /usr/share/crunch/charset.lst lalpha -t @@admin@@ > dicionario.txt

Password Cracking



Password Cracking

DICIONÁRIOS NO KALI

/usr/share/john/password.lst

/usr/share/metasploit-framework/data/wordlists/password.lst

/usr/share/wordlists/rockyou.txt

Diretório: /usr/share/wordlists

Windows Passwords

Password Cracking

Lan Manager(LM) foi uns dos primeiros algoritmos de hash de senhas utilizados em sistemas Microsoft Windows. A sua evolução o NTLM, foi implementada apartir do Windows 2000, XP, Vista, Seven. Por padrão foi mantido compatibilidade com o antigo LM, porém no Windows Vista e Seven, a compatibilidade com o LM é desativada.

O arquivo (SAM) que guarda as credenciais do Microsoft Windows fica no caminho C:\Windows\system32\config\

Esse arquivo ele é bloqueado pelo sistema durante a execução do mesmo (syskey). Para cópia utiliza-se um Live-CD para acessar o HD, ou ainda programas como fgdump para extrair os hashes das senhas do usuários.

Administrator:500:NO PASSWORD**********:NO PASSWORD**********:::
CbSampaio:1007:4BC4A78F7366139DAAD3B435B51404EE:66BC75EF4487330DD21B56AEBD0A1B28:::
Guest:501:NO PASSWORD**********:NO PASSWORD**********:::
HelpAssistant:1000:D95093A47C269488861DAC097CE62A78:F1E06A7E7A168A58C975EC1D430FC020:::
MajCarlos:1004:598DDCE2660D3193AAD3B435B51404EE:2D20D252A479F485CDF5E171D93985BF:::
SdVieira:1008:6089B6316B3577C4944E2DF489A880E4:68365827D79C4F5CC9B52B688495FD51:::
SgtRafael:1006:BCFFF673D5C8F5FE1D71060D896B7A46:1347038829874A200B2680591E25940A:::
SUPPORT_388945a0:1002:NO PASSWORD**********:98F57B7B417BEFF502B51903B25958DD:::
TenHumberto:1005:147DE9A4F811A03AAAD3B435B51404EE:4228BEA7BC5EF7447FB29541A268B65B:::

Password Cracking

Algoritmo de hash LM → 6 passos.

1)Todas as letras da senha são convertidas para MAIÚSCULAS.
2)A senha é completadas com valores nulos até completar 14 caracteres.
3)A senha é dividida em duas partes de 7 caracteres cada.
4)Cada parte é utilizada para criar uma chave criptográfica DES onde é adicionado um bit de paridade nas duas partes formando chaves de 64 bits.
5)Cada chave DES é utilizada para criptografar o texto (KGS!@#$%) resultando em 8 bytes de texto crifrado.
6)As duas parte cifradas foram o LM hash de 16 bytes.

Ex: Senha → PaSsWoRd123

1)PASSWORD123
2)PASSWORD123000
3)PASSWOR and D123000
4)PASSWOR1 and D1230001
5)E52CAC67419A9A22 and 664345140A852F61
6)E52CAC67419A9A22664345140A852F61

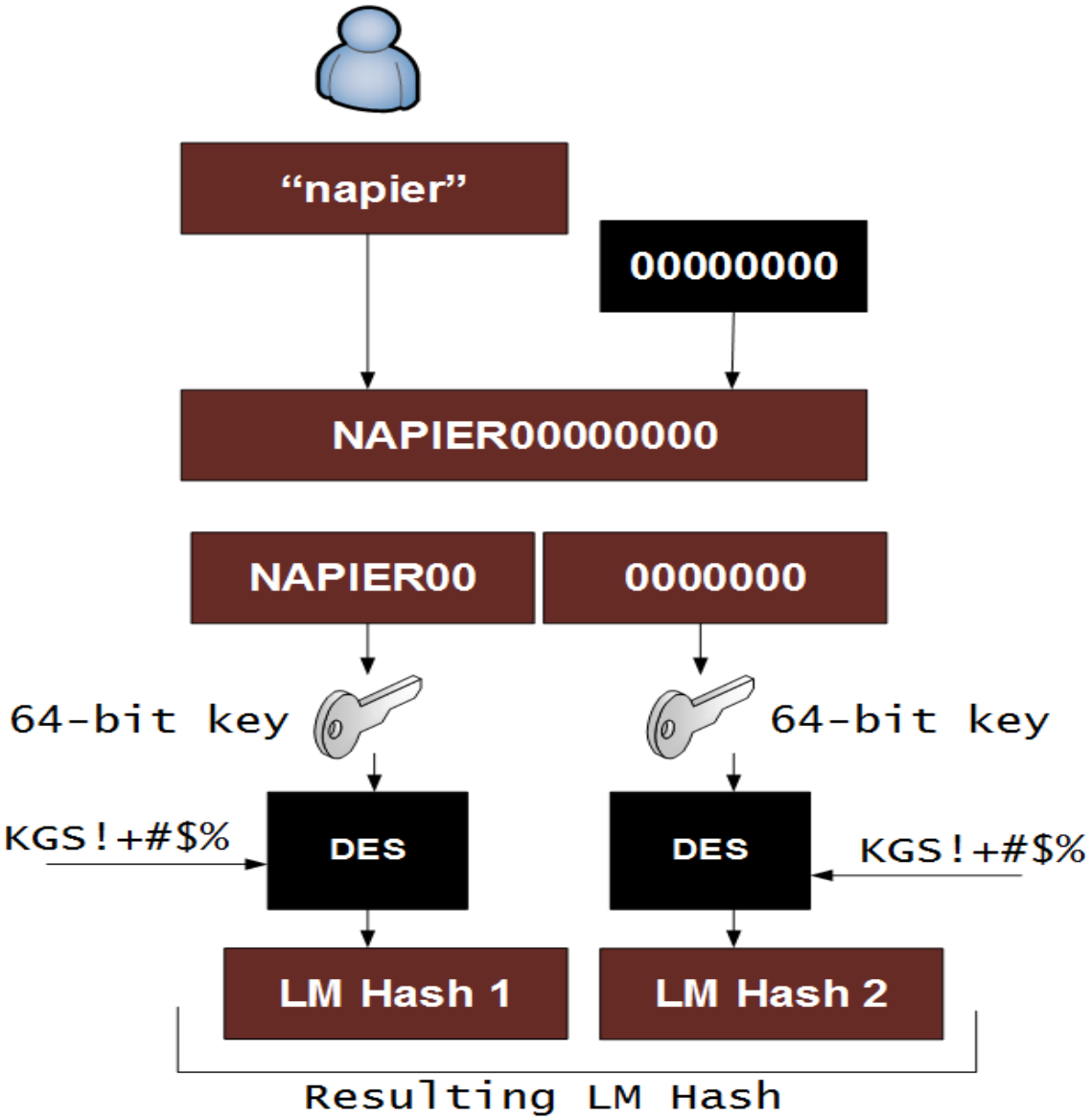
Password Cracking

Algoritmo de hash NTLM

- Utiliza o MD4 para algoritmo de hash(ja encontrado vulnerabilidades nesse algoritmo)
- Permite utilizar letras maiúsculas e minusculas o que o LM não permitia.
- NÃO IMPLEMENTA SALT

https://crackstation.net/
https://www.objectif-securite.ch/en/ophcrack.php
http://ophcrack.sourceforge.net/

Password Cracking



Password Cracking

Shiela/test

Password hash using LM/NTLM

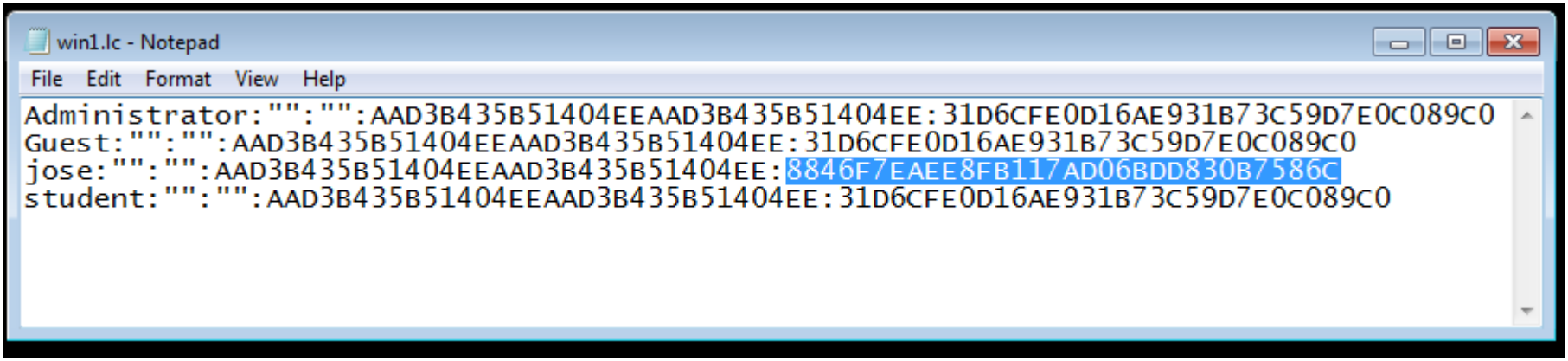
```
Shiela:1005:NO PASSWORD****
**********************:0CB694880
5F797BF2A82807973B89537:::
```

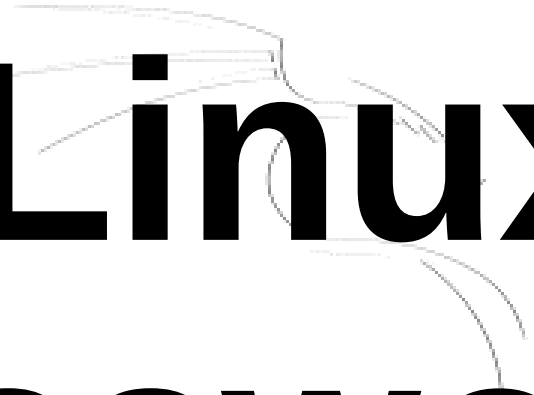
SAM File is located at `c:\windows\system32\config\SAM`

```
Administrator:500:NO PASSWORD**********************:61880B9EE373475C8148A7108ACB3031:::
Guest:501:NO PASSWORD**********************:NO PASSWORD**********************:::
Admin:1001:NO PASSWORD**********************:BE40C450AB99713DF1EDC5B40C25AD47:::
Martin:1002:NO PASSWORD**********************:BF4A502DA294ACBC175B394A080DEE79:::
Juggyboy:1003:NO PASSWORD**********************:488CDCDD2225312793ED6967B28C1025:::
Jason:1004:NO PASSWORD**********************:2D20D252A479F485CDF5E171D93985BF:::
Shiela:1005:NO PASSWORD**********************:0CB6948805F797BF2A82807973B89537:::
```

User name | User ID | LM Hash | NTLM Hash

Password Cracking





Linux Passwords

Password Cracking

Toda conta no sistema Linux tem uma entrada no arquivo '/etc/passwd'. Este arquivo contém entradas, uma linha por usuário, que especificam diversos atributos para cada conta. Cada entrada neste arquivo tem o mesmo formato, com campos separados por "dois pontos":

usuário:senha:UID:GID:NomeReal:/diretório/pessoal:shell

Exemplo de arquivo '/etc/passwd':

root:**x**:0:0:root:/root:/bin/bash
ftp:**x**:14:50:FTP User:/var/ftp:/sbin/nologin
postgres:**x**:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
fulano:**x**:500:500:Fulano da Silva:/home/fulano:/bin/bash
siclano:**x**:501:501:Siclano Souza:/home/siclano:/bin/bash

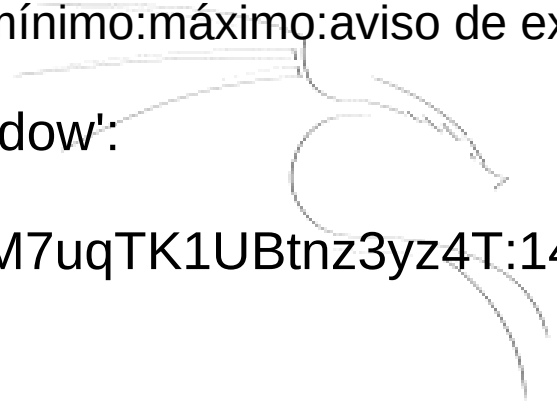
“**x**”: hash da senha omitida, conteúdo no arquivo /etc/shadow

Password Cracking

O arquivo '/etc/shadow' armazena as senhas em um formato criptografado, com algumas informações adicionais relacionadas as senhas dos usuários. Contém uma entrada por linha, separada em campos, para cada usuário definido no '/etc/passwd'.

usuário:senha:última alteração:mínimo:máximo:aviso de expiração:inativo:expiração:

Exemplo de arquivo '/etc/shadow':



root:6utLIMf6gY40$Eoe.2M7uqTK1UBtnz3yz4T:14768:0:99999:7:::
daemon:*:14715:0:99999:7:::
lp:*:14715:0:99999:7:::
shutdown:*:14715:0:99999:7:::
ftp:*:14715:0:99999:7:::
nobody:*:14715:0:99999:7:::
postgres:!!:14855::::::
fulano:6nsd3oKxkg0$kIEvBac347MZXYfOnrc56ybz:14768:0:99999:7:::
siclano:6AaNgoXJSPsv/$cupVfet0y4cIYLpPSWyNQM:14771:0:99999:7:::
beltrano:6Qc3AYPleBx0$ikGowHMwzkqRz9QGZzQfwfu:14770:0:99999:7:::

Password Cracking

A string completa com o hash, que representa a senha, é armazenada no arquivo '/etc/shadow' no formato **IDSALT$SENHA**. O caractere "$" (cifrão) delimita cada item da string. Por exemplo a linha a seguir (Nota: há uma quebra de linha no meio do hash para facilitar a apresentação, no arquivo é somente uma única linha):

nome_do_usuário:
$**6**$**eKn9QGMQ**$**Ofi1OoClVpw/cCbTsD4YUKgfurcQoBxsZ9Tlk5VBjTp**
AjSYFt.M9shPtQVnouNr4/3PRDP/eMqkoWQpuBxsRk1:15362:0:99999:7:::

UNSHADOW

unshadow <arq passwd> <arq shadow> > <arquivo>

unshadow /etc/passwd /etc/shadow > unshadow

Brute Force

Password Cracking

Comando:

hydra -l <login> -p <senha> <IP> <serviço> -t <tasks>
hydra -l root -p 12345 10.0.2.2 ssh -t 8

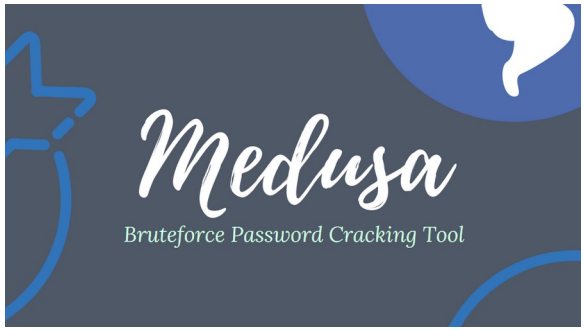
Podemos passar um dicionário de logins e senhas com o parâmetro -L e -P

hydra -L <arquivo_login> -P <arquivo_senha> <IP> <serviço>
hydra -L login.txt -P senha.txt 10.0.2.2 ssh -t 4

Interface Grafica:

xhydra

Password Cracking



Para listar os módulos

```
medusa -q | more
```

Comando:

```
medusa -h <ip> -u <usuario> -p <senha> -M <modulo>
medusa -h 10.10.100.25 -u admin -p 1234 -M ftp
```

Lista de IP, usuários e senhas

```
medusa -H <ips> -U <usuarios> -P <senhas> -M <modulo>
medusa -H hosts.txt -U users.txt -P pass.txt -M smbnt
```

Password Cracking

John the Ripper é um utilitário que faz quebra de senhas através de três modos:

- **WordList** → Ele tenta por uma Wordlist, testando as combinações de senha/usuário.
- **Single Crack** → Ele tenta quebrar a senha usando as informações de login.
- **Incremental** → Sendo o modo mais robusto no John the Ripper, ele tentará cada caractere possível até achar a senha correta. E por este motivo, é indicado o uso de parâmetros com o intuito de reduzir o tempo de quebra.

Password Cracking

Comando:

john <arquivo> --wordlist=dicionario.txt
john <arquivo> --single
john <arquivo> --incremental

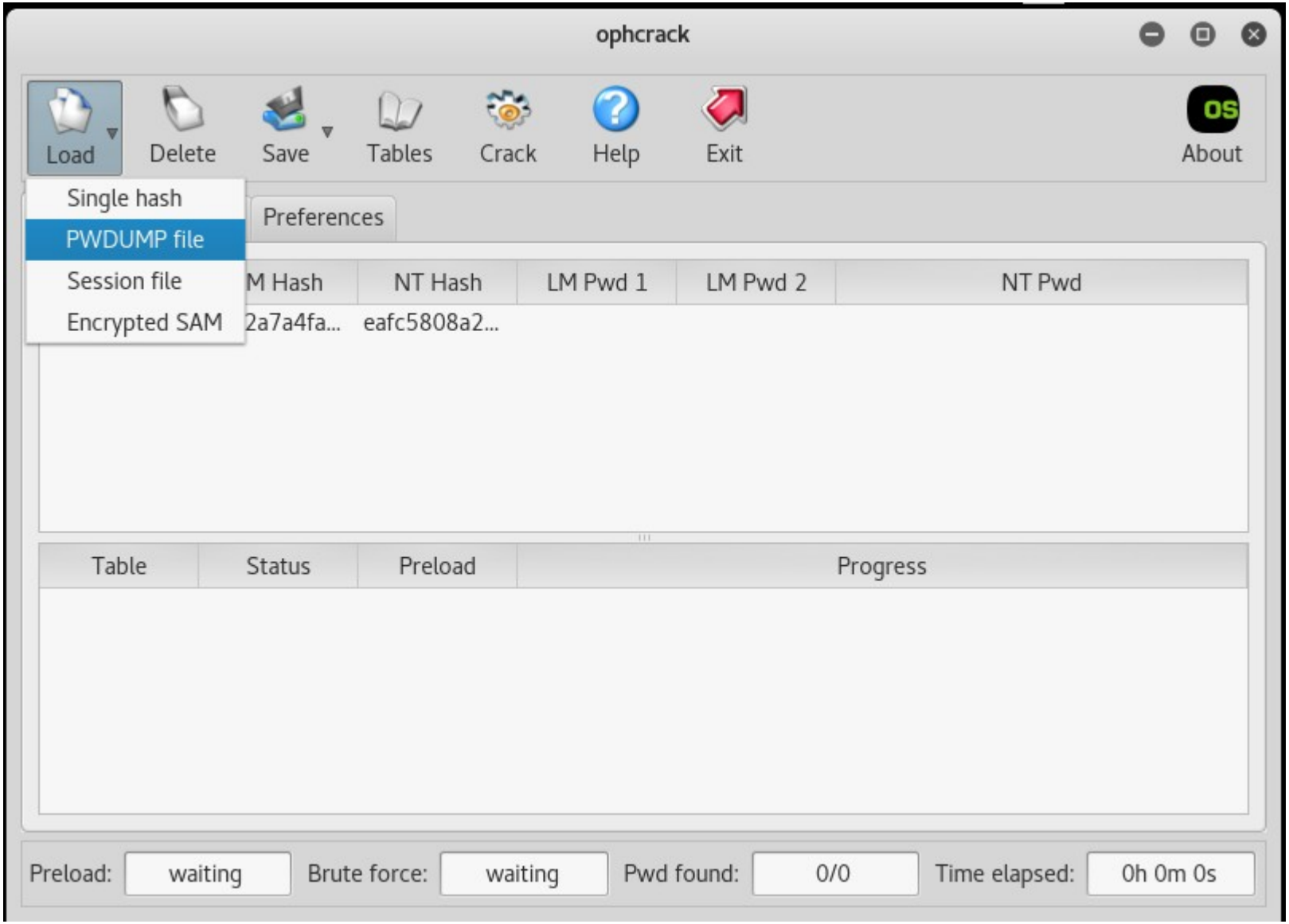
john <arquivo> --wordlist=dicionario.txt --format=NT

Senhas quebradas são armazenadas no arquivo:
<home_do_usuário)>/.john/john.pot

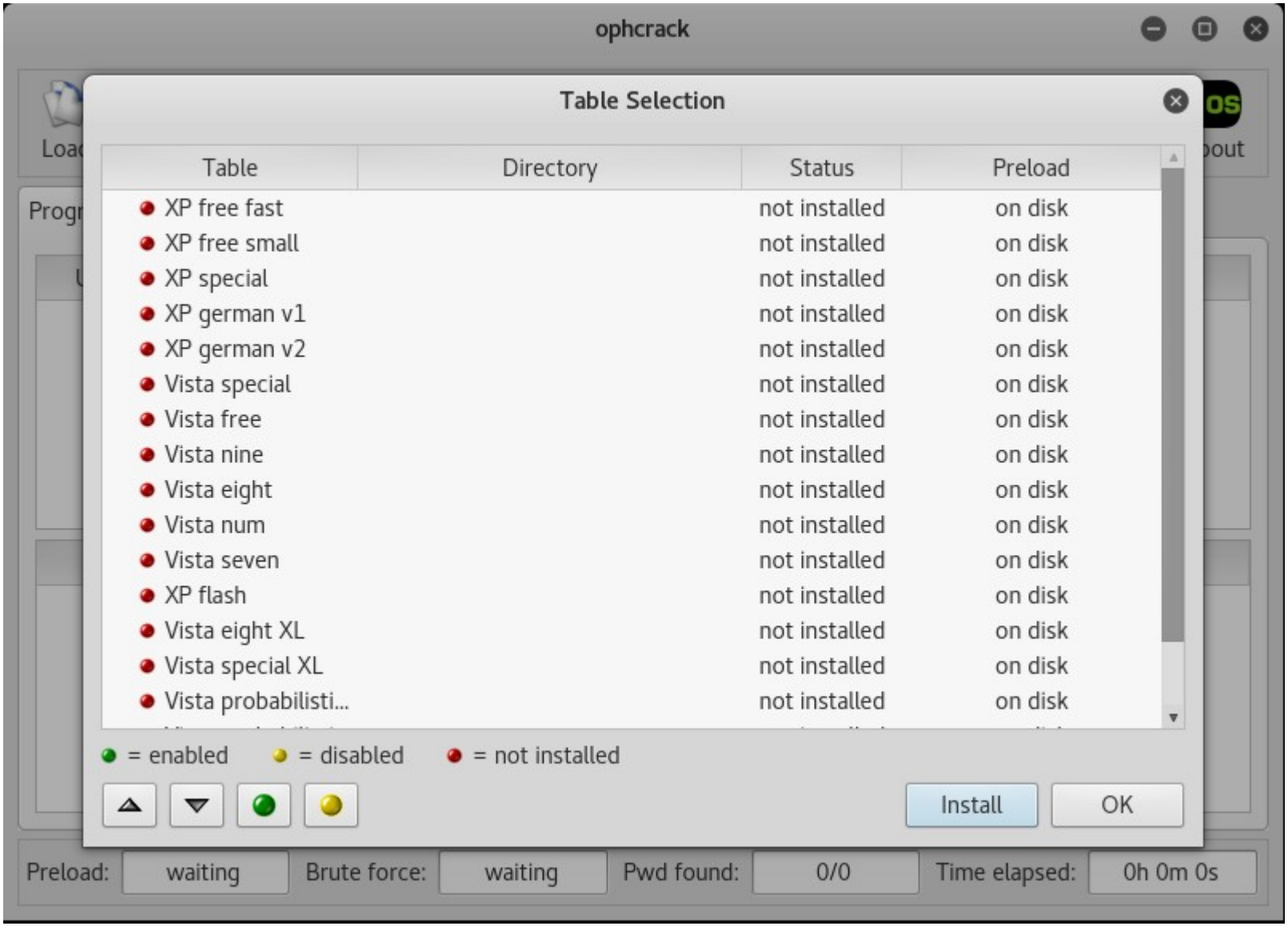
Interface Grafica:

johnny

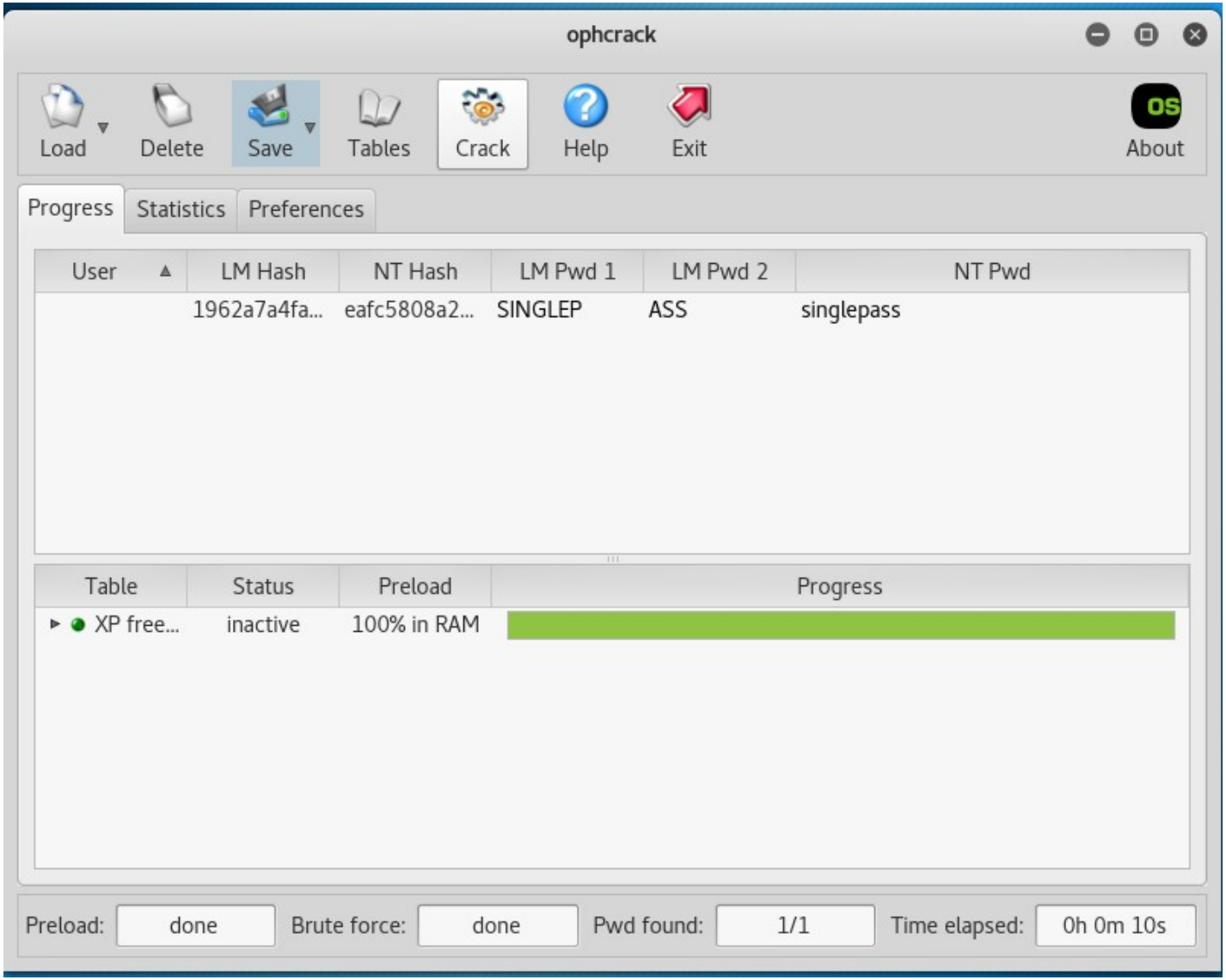
Password Cracking



Password Cracking

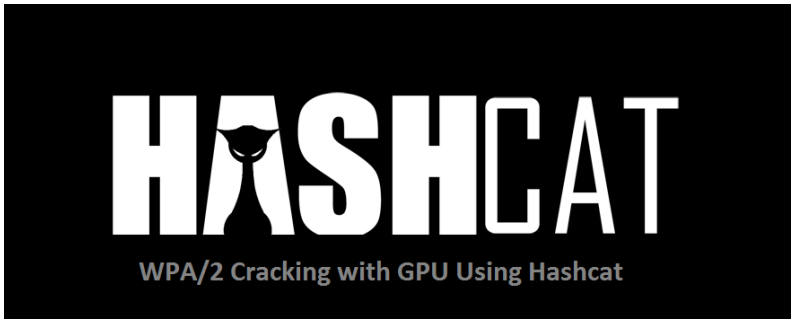


Password Cracking



Password Cracking

Exemplo utilizando dicionário



hashcat -m <tipo do hash> -a <tipo do ataque> -o <arquivo de saída> <arquivo de hash> <dicionário>

hashcat -m 1800 -a 0 -o cracked.txt /etc/shadow /usr/share /usr/share/wordlists/rockyou.txt

- Caso os drivers da placa de video não estejam instalados é necessário utilizar a opção --force

hashcat -m 1800 -a 0 -o cracked.txt /etc/shadow /usr/share /usr/share/wordlists/rockyou.txt --force

Password Cracking